

#3

P20745.P04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :M. AKIMOTO et al.

Serial No. :Not Yet Assigned

Filed :Concurrently Herewith

For :A COMMUNICATION CONTROL APPARATUS AND A COMMUNICATION
CONTROL METHOD

CLAIM OF PRIORITY

Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

Applicant hereby claims the right of priority granted pursuant to 35 U.S.C. 119 based upon Japanese Application No. 2000-236917, filed August 4, 2000. As required by 37 C.F.R. 1.55, a certified copy of the Japanese application is being submitted herewith.

Respectfully submitted,
M. AKIMOTO et al.

Leslie J. Paperner Reg. No.
Bruce H. Bernstein
Reg. No. 29,027 *33,329*

August 2, 2001
GREENBLUM & BERNSTEIN, P.L.C.
1941 Roland Clarke Place
Reston, VA 20191
(703) 716-1191



日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

J1050 U.S. PTO
09/919953
08/02/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 8月 4日

出 願 番 号

Application Number:

特願2000-236917

出 願 人

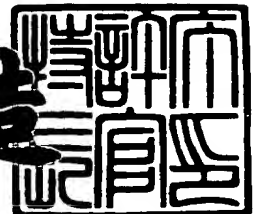
Applicant (s):

松下電送システム株式会社

2001年 3月 2日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3015384

【書類名】 特許願

【整理番号】 2952020019

【提出日】 平成12年 8月 4日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/00

【発明者】

【住所又は居所】 東京都目黒区下目黒2丁目3番8号 松下電送システム
株式会社内

【氏名】 秋元 正男

【発明者】

【住所又は居所】 東京都目黒区下目黒2丁目3番8号 松下電送システム
株式会社内

【氏名】 村田 松寿

【特許出願人】

【識別番号】 000187736

【氏名又は名称】 松下電送システム株式会社

【代理人】

【識別番号】 100105050

【弁理士】

【氏名又は名称】 鷲田 公一

【手数料の表示】

【予納台帳番号】 041243

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9603473

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 通信制御装置及び通信制御方法

【特許請求の範囲】

【請求項 1】 インターネットファクシミリ装置に接続される第 1 インタフェース部と、前記インターネットファクシミリ装置が接続され、サーバ装置により HTTP プロトコルで管理されるネットワークに接続される第 2 インタフェース部と、前記インターネットファクシミリ装置との間で SMTP プロトコルに従って通信を制御する SMTP 処理部と、前記サーバ装置との間で HTTP プロトコルに従って通信を制御する HTTP 処理部と、前記インターネットファクシミリ装置から電子メールデータを受信する電子メール通信部と、前記電子メールデータを HTML データに変換する HTML 処理部と、前記 HTML データを前記サーバ装置に送信する HTML 通信部と、を具備することを特徴とする通信制御装置。

【請求項 2】 前記第 1 インタフェース部を介して送信される信号種別を判定する信号種別判定部を具備し、前記信号種別判定部が前記インターネットファクシミリ装置から所定の信号種別を判定した場合、前記 HTTP 処理部は、前記サーバ装置との間で HTTP プロトコルに従って通信の制御を開始する一方、前記 SMTP 処理部は、前記インターネットファクシミリ装置との間で SMTP プロトコルに従って通信を制御することを特徴とする請求項 1 記載の通信制御装置。

【請求項 3】 前記 HTTP 処理部は、前記信号種別判定部が前記インターネットファクシミリ装置から SMTP プロトコルに従ったコマンド信号である「HELO」を受信した場合に前記サーバ装置との間で HTTP プロトコルに従って通信の制御を開始することを特徴とする請求項 2 記載の通信制御装置。

【請求項 4】 前記電子メール通信部が受信した電子メールデータに対して暗号化処理を行う暗号化処理部を具備し、前記 HTML 処理部は、前記暗号化処理部が暗号化処理を施した電子メールデータを HTML データに変換することを特徴とする請求項 1 から請求項 3 のいずれかに記載の通信制御装置。

【請求項 5】 前記暗号化処理部の暗号化処理に必要となる情報を格納する

ICカードと、前記ICカードが挿入されるスロット部と、を具備し、前記暗号化処理部は、前記スロット部に前記ICカードが挿入されている場合に当該ICカード内の前記情報を用いて暗号化処理を行うことを特徴とする請求項4記載の通信制御装置。

【請求項6】 インターネットファクシミリ装置に接続される第1インタフェース部と、前記インターネットファクシミリ装置が接続され、サーバ装置によりHTTPプロトコルで管理されるネットワークに接続される第2インタフェース部と、前記インターネットファクシミリ装置との間でPOP3プロトコルに従って通信を制御するPOP3処理部と、前記サーバ装置との間でHTTPプロトコルに従って通信を制御するHTTP処理部と、前記サーバ装置から電子メールデータを含むHTMLデータを受信するHTML通信部と、前記HTMLデータから電子メールデータを取り出すHTML処理部と、前記インターネットファクシミリ装置に前記電子メールデータを送信する電子メール通信部と、を具備することを特徴とする通信制御装置。

【請求項7】 前記第1インタフェース部を介して送信される信号種別を判定する信号種別判定部を具備し、前記信号種別判定部が前記インターネットファクシミリ装置から所定の信号種別を判定した場合、前記HTTP処理部は、前記サーバ装置との間でHTTPプロトコルに従って通信の制御を開始する一方、前記POP3処理部は、前記インターネットファクシミリ装置との間でPOP3プロトコルに従って通信を制御することを特徴とする請求項6記載の通信制御装置。

【請求項8】 前記HTTP処理部は、前記信号種別判定部が前記インターネットファクシミリ装置からPOP3プロトコルに従ったコマンド信号である「USER」を受信した場合に前記サーバ装置との間でHTTPプロトコルに従って通信の制御を開始することを特徴とする請求項7記載の通信制御装置。

【請求項9】 前記HTML処理部がHTMLデータから取り出した電子メールデータに暗号化処理が施されている場合に復号化処理を行う復号化処理部を具備し、前記電子メール通信部は、前記復号化処理部が復号化処理を行った電子メールデータを前記インターネットファクシミリ装置に送信することを特徴とす

る請求項 6 から請求項 8 のいずれかに記載の通信制御装置。

【請求項 1 0】 前記復号化処理部の復号化処理に必要となる情報を格納する IC カードと、前記 IC カードが挿入されるスロット部と、を具備し、前記復号化処理部は、前記スロット部に前記 IC カードが挿入されている場合に当該 IC カード内の前記情報を用いて復号化処理を行うことを特徴とする請求項 9 記載の通信制御装置。

【請求項 1 1】 前記 IC カードは、電子メールアドレス情報を格納し、前記 HTML 通信部は、前記スロット部に前記 IC カードが挿入されている場合に当該 IC カード内の前記電子メールアドレス情報に着信した電子メールデータに対応する HTML データを受信することを特徴とする請求項 1 0 記載の通信制御装置。

【請求項 1 2】 インターネットファクシミリ装置に接続される第 1 インタフェース部から SMTP プロトコルに従った所定の信号種別を判定する工程と、前記所定の信号種別を判定した場合に前記インターネットファクシミリ装置との間で SMTP プロトコルに従って通信を制御する一方、前記インターネットファクシミリ装置が接続され、サーバ装置により HTTP プロトコルで管理されるネットワークに接続される第 2 インタフェース部を介して前記サーバ装置との間で HTTP プロトコルに従って通信を制御する工程と、前記インターネットファクシミリ装置から電子メールデータを受信する工程と、前記電子メールデータを HTML データに変換する工程と、前記 HTML データを前記サーバ装置に送信する工程と、を具備することを特徴とする通信制御方法。

【請求項 1 3】 インターネットファクシミリ装置に接続される第 1 インタフェース部から POP 3 プロトコルに従った所定の信号種別を判定する工程と、前記所定の信号種別を判定した場合に前記インターネットファクシミリ装置との間で POP 3 プロトコルに従って通信を制御する一方、前記インターネットファクシミリ装置が接続され、サーバ装置により HTTP プロトコルで管理されるネットワークに接続される第 2 インタフェース部を介して前記サーバ装置との間で HTTP プロトコルに従って通信を制御する工程と、前記サーバ装置から電子メールデータを含む HTML データを受信する工程と、前記 HTML データから電

子メールアドレスを取り出す工程と、取り出した前記電子メールアドレスを前記インターネットファクシミリ装置に送信する工程と、を具備することを特徴とする通信制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、インターネットファクシミリ装置とネットワークとの間に接続され、双方の間で通信制御を行う通信制御装置及び通信制御方法に関する。

【0002】

【従来の技術】

従来、企業などの組織内の情報共有を効率的に行うためにグループウェアソフトを利用してネットワークを構築することが行われている。近年、このようなネットワーク（以下、「グループウェアネットワーク」という）には、インターネット技術を取り入れ、WWWブラウザから利用可能なグループウェアソフトが採用されることが多い。この場合、そのグループウェアネットワーク上のPC等のクライアント端末は、WWWブラウザを利用することで、グループウェアネットワーク上で情報を共有することができる。これにより、クライアント端末は、電子メールや電子掲示板等の機能を実現することができる。

【0003】

一方、近年、一般的なファクシミリと同様の操作で画情報をインターネット経由で送信するファクシミリ装置が開発されている。この種のファクシミリは、通信経路の全部又は一部にインターネットを使用することからインターネットファクシミリ装置（以下、「IFAX」という）と呼ばれている。このようなIFAXは、画情報の送信時は、ファクシミリデータを電子メールのフォーマットに変換して送信する。一方、画情報の受信時は、受信した電子メールアドレスをファクシミリのフォーマットに変換して印刷処理を行う。このとき、IFAXは、電子メールアドレスの通信をSMTP（Simple Mail Transfer Protocol）やPOP3（Post Office Protocol Version3）等のプロトコルに従って制御している。

【0004】

【発明が解決しようとする課題】

しかしながら、上述のようなWWWブラウザを利用したグループウェアネットワークにおいては、各種データは、HTTPプロトコルに従って通信が行われる。このため、SMTP (Simple Mail Transfer Protocol) やPOP3 (Post Office Protocol Version3) に従って通信を制御するIFAXは、動作することができないという問題がある。

【0005】

本発明は、かかる点に鑑みてなされたものであり、HTTPプロトコルで管理されたネットワーク上でもIFAXを正常に動作させることができる通信制御装置及び通信制御方法を提供することを目的とする。

【0006】

【課題を解決するための手段】

本発明は、IFAXに接続される第1インタフェース部からSMTPプロトコルに従った所定の信号種別を判定し、所定の信号種別を判定した場合にIFAXとの間でSMTPプロトコルに従って通信を制御する一方、IFAXが接続され、サーバ装置によりHTTPプロトコルで管理されるネットワークに接続される第2インタフェース部を介して、サーバ装置との間でHTTPプロトコルに従って通信を制御しながら、IFAXから電子メールデータを受信し、受信した電子メールデータをHTMLデータに変換し、さらにそのHTMLデータをサーバ装置に送信するようにしたものである。

【0007】

これにより、IFAXからサーバ装置に電子メールを送信する際、IFAXとの間でSMTPに従って各種信号や電子メールデータの通信を行う一方、サーバ装置との間でHTTPプロトコルに従って各種信号や電子メールデータの通信を行う。このため、HTTPプロトコルで管理されるネットワークにおいても、IFAXは、正常に電子メールの送信動作を行うことができる。

【0008】

また、本発明は、IFAXに接続される第1インタフェース部からPOP3プロトコルに従った所定の信号種別を判定し、所定の信号種別を判定した場合にI

FAXとの間でPOP3プロトコルに従って通信を制御する一方、IFAXが接続され、サーバ装置によりHTTPプロトコルで管理されるネットワークに接続される第2インタフェース部を介して、サーバ装置との間でHTTPプロトコルに従って通信を制御しながら、サーバ装置から電子メールデータを含むHTMLデータを受信し、受信したHTMLデータから電子メールデータを取り出し、取り出した電子メールデータをIFAXに送信するようにしたものである。

【0009】

これにより、IFAXがサーバ装置から電子メールを受信する際、IFAXとの間でPOP3プロトコルに従って各種信号や電子メールデータの通信を行う一方、サーバ装置との間でHTTPプロトコルに従って各種信号や電子メールデータの通信を行う。このため、HTTPプロトコルで管理されたネットワークにおいても、IFAXは、正常に電子メールの受信動作を行うことができる。

【0010】

【発明の実施の形態】

本発明の第1の態様に係る通信制御装置は、インターネットファクシミリ装置に接続される第1インタフェース部と、前記インターネットファクシミリ装置が接続され、サーバ装置によりHTTPプロトコルで管理されるネットワークに接続される第2インタフェース部と、前記インターネットファクシミリ装置との間でSMTPプロトコルに従って通信を制御するSMTP処理部と、前記サーバ装置との間でHTTPプロトコルに従って通信を制御するHTTP処理部と、前記インターネットファクシミリ装置から電子メールデータを受信する電子メール通信部と、前記電子メールデータをHTMLデータに変換するHTML処理部と、前記HTMLデータを前記サーバ装置に送信するHTML通信部と、を具備する構成を採る。

【0011】

この構成によれば、IFAXからサーバ装置に電子メールを送信する際、IFAXとの間でSMTPプロトコルに従って各種信号や電子メールデータの通信を行う一方、サーバ装置との間でHTTPプロトコルに従って各種信号や電子メールデータの通信を行う。このため、HTTPプロトコルで管理されるネットワー

クにおいても、I F A Xは、正常に電子メールの送信動作を行うことができる。

【 0 0 1 2 】

本発明の第2の態様に係る通信制御装置は、第1の態様において、前記第1インタフェース部を介して送信される信号種別を判定する信号種別判定部を具備し、前記信号種別判定部が前記インターネットファクシミリ装置から所定の信号種別を判定した場合、前記H T T P処理部は、前記サーバ装置との間でH T T Pプロトコルに従って通信の制御を開始する一方、前記S M T P処理部は、前記インターネットファクシミリ装置との間でS M T Pプロトコルに従って通信を制御する構成を採る。

【 0 0 1 3 】

本発明の第3の態様に係る通信制御装置は、第2の態様において、前記H T T P処理部は、前記信号種別判定部が前記インターネットファクシミリ装置からS M T Pプロトコルに従ったコマンド信号である「H E L O」を受信した場合に前記サーバ装置との間でH T T Pプロトコルに従って通信の制御を開始する構成を採る。

【 0 0 1 4 】

これらの構成によれば、インターネットファクシミリ装置から所定の信号（第3の態様では、「H E L O」）を受信した場合に、H T T P処理部がサーバ装置とH T T Pプロトコルに従って通信制御を行う。これと並行して、S M T P処理部がインターネットファクシミリ装置とS M T Pプロトコルに従って通信制御を行う。このため、インターネットファクシミリ装置とサーバ装置との間において、リアルタイムで通信制御を行うことができる。これにより、いずれか一方との通信を完了した後に他方と通信を開始するような場合に発生する事態を防止することができる。例えば、送信済みデータを削除することによって、同一データの再送ができないような事態が防止される。なお、ここでは、第3の態様で「H E L O」を具体例として説明しているが、これ以外のS M T Pプロトコルに従ったコマンド信号（例えば、「M A I L」、「R C P T」等）であってもよい。

【 0 0 1 5 】

本発明の第4の態様に係る通信制御装置は、第1から第3のいずれかの態様に

において、前記電子メール通信部が受信した電子メールデータに対して暗号化処理を行う暗号化処理部を具備し、前記HTML処理部は、前記暗号化処理部が暗号化処理を施した電子メールデータをHTMLデータに変換する構成を採る。

【0016】

この構成によれば、暗号化処理部がその暗号化処理を施した電子メールデータがHTMLデータに変換されてサーバ装置に送信される。これにより、HTTPプロトコルで管理されるネットワークにおいても、IFAXは、正常に電子メールの送信動作を行うことができると共に、既存のインターネットファクシミリ装置に特別な構成を附加することなく、インターネットファクシミリ装置から送信される電子メールの秘匿性を確保することができる。

【0017】

本発明の第5の態様に係る通信制御装置は、第4の態様において、前記暗号化処理部の暗号化処理に必要となる情報を格納するICカードと、前記ICカードが挿入されるスロット部と、を具備し、前記暗号化処理部は、前記スロット部に前記ICカードが挿入されている場合に当該ICカード内の前記情報を用いて暗号化処理を行う構成を採る。

【0018】

この構成によれば、ICカードがスロット部に挿入されている場合にのみ、その内部に格納された情報に基づいて暗号化処理が施されるため、簡単に暗号化処理の可否を判断することができる。

【0019】

本発明の第6の態様に係る通信制御装置は、インターネットファクシミリ装置に接続される第1インタフェース部と、前記インターネットファクシミリ装置が接続され、サーバ装置によりHTTPプロトコルで管理されるネットワークに接続される第2インタフェース部と、前記インターネットファクシミリ装置との間でPOP3プロトコルに従って通信を制御するPOP3処理部と、前記サーバ装置との間でHTTPプロトコルに従って通信を制御するHTTP処理部と、前記サーバ装置から電子メールデータを含むHTMLデータを受信するHTML通信部と、前記HTMLデータから電子メールデータを取り出すHTML処理部と、

前記インターネットファクシミリ装置に前記電子メールアドレスを送信する電子メール通信部と、を具備する構成を採る。

【 0 0 2 0 】

この構成によれば、I F A Xがサーバ装置から電子メールを受信する際、I F A Xとの間でP O P 3 プロトコルに従って各種信号や電子メールアドレスの通信を行う一方、サーバ装置との間でH T T P プロトコルに従って各種信号や電子メールアドレスの通信を行う。このため、H T T P プロトコルで管理されたネットワークにおいても、I F A Xは、正常に電子メールの受信動作を行うことができる。

【 0 0 2 1 】

本発明の第7の態様に係る通信制御装置は、第6の態様において、前記第1インタフェース部を介して送信される信号種別を判定する信号種別判定部を具備し、前記信号種別判定部が前記インターネットファクシミリ装置から所定の信号種別を判定した場合、前記H T T P 処理部は、前記サーバ装置との間でH T T P プロトコルに従って通信の制御を開始する一方、前記P O P 3 処理部は、前記インターネットファクシミリ装置との間でP O P 3 プロトコルに従って通信を制御する構成を採る。

【 0 0 2 2 】

本発明の第8の態様に係る通信制御装置は、第7に態様において、前記H T T P 処理部は、前記信号種別判定部が前記インターネットファクシミリ装置からP O P 3 プロトコルに従ったコマンド信号である「U S E R」を受信した場合に前記サーバ装置との間でH T T P プロトコルに従って通信の制御を開始する構成を採る。

【 0 0 2 3 】

これらの構成によれば、インターネットファクシミリ装置から所定の信号（第8の態様では、「U S E R」）を受信した場合に、H T T P 処理部がサーバ装置とH T T P プロトコルに従って通信制御を行う。これと並行して、P O P 3 処理部がインターネットファクシミリ装置とP O P プロトコルに従って通信制御を行う。このため、インターネットファクシミリ装置とサーバ装置との間において、リアルタイムで通信制御を行うことができる。これにより、いずれか一方との通

信を完了した後に他方と通信を開始するような場合に発生する事態を防止することができる。

【 0 0 2 4 】

本発明の第 9 の態様に係る通信制御装置は、第 6 から第 8 のいずれかの態様において、前記 HTML 処理部が HTML データから取り出した電子メールデータに暗号化処理が施されている場合に復号化処理を行う復号化処理部を具備し、前記電子メール通信部は、前記復号化処理部が復号化処理を行った電子メールデータを前記インターネットファクシミリ装置に送信する構成を採る。

【 0 0 2 5 】

この構成によれば、HTML データから取り出した電子メールデータに暗号化処理が施されている場合、復号化処理が行われた電子メールデータがインターネットファクシミリ装置に送信される。これにより、HTTP プロトコルで管理されたネットワークにおいても、IFAX は、正常に電子メールの受信動作を行うことができると共に、既存のインターネットファクシミリ装置に特別な構成を附加することなく、インターネットファクシミリ装置から送信される電子メールの秘匿性を確保することができる。

【 0 0 2 6 】

本発明の第 1 0 の態様に係る通信制御装置は、第 9 の態様において、前記復号化処理部の復号化処理に必要となる情報を格納する IC カードと、前記 IC カードが挿入されるスロット部と、を具備し、前記復号化処理部は、前記スロット部に前記 IC カードが挿入されている場合に当該 IC カード内の前記情報を用いて復号化処理を行う構成を採る。

【 0 0 2 7 】

この構成によれば、IC カードがスロット部に挿入されている場合にのみ、その内部に格納された情報に基づいて復号化処理が施されるため、簡単に復号化処理の可否を判断することができる。

【 0 0 2 8 】

本発明の第 1 1 の態様に係る通信制御装置は、第 1 0 の態様において、前記 IC カードは、電子メールアドレス情報を格納し、前記 HTML 通信部は、前記ス

ロット部に前記ＩＣカードが挿入されている場合に当該ＩＣカード内の前記電子メールアドレス情報に着信した電子メールデータに対応するＨＴＭＬデータを受信する構成を採る。

【 0 0 2 9 】

この構成によれば、電子メール通信部は、ＩＣカードがスロット部に挿入されている場合にのみ電子メールデータの受信処理を行う。このとき、電子メールデータの受信処理は、そのＩＣカード内に格納された電子メールアドレス情報を用いて行われる。このため、接続されたインターネットファクシミリ装置を多人数で使用する場合においても、自分のメールアドレスに届いた電子メールデータを他人に見られることなく受信することができる。これにより、他人に自分宛ての電子メールデータを見られるという事態を防止することができ、より電子メールデータの秘匿性を確保することができる。

【 0 0 3 0 】

本発明の第１２の態様に係る通信制御方法は、インターネットファクシミリ装置に接続される第１インタフェース部からＳＭＴＰプロトコルに従った所定の信号種別を判定する工程と、前記所定の信号種別を判定した場合に前記インターネットファクシミリ装置との間でＳＭＴＰプロトコルに従って通信を制御する一方、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰプロトコルで管理されるネットワークに接続される第２インタフェース部を介して前記サーバ装置との間でＨＴＴＰプロトコルに従って通信を制御する工程と、前記インターネットファクシミリ装置から電子メールデータを受信する工程と、前記電子メールデータをＨＴＭＬデータに変換する工程と、前記ＨＴＭＬデータを前記サーバ装置に送信する工程と、を具備するようにしたものである。

【 0 0 3 1 】

本発明の第１３の態様に係る通信制御方法は、インターネットファクシミリ装置に接続される第１インタフェース部からＰＯＰ３プロトコルに従った所定の信号種別を判定する工程と、前記所定の信号種別を判定した場合に前記インターネットファクシミリ装置との間でＰＯＰ３プロトコルに従って通信を制御する一方、前記インターネットファクシミリ装置が接続され、サーバ装置によりＨＴＴＰ

プロトコルで管理されるネットワークに接続される第2インタフェース部を介して前記サーバ装置との間でHTTPプロトコルに従って通信を制御する工程と、前記サーバ装置から電子メールデータを含むHTMLデータを受信する工程と、前記HTMLデータから電子メールデータを取り出す工程と、取り出した前記電子メールデータを前記インターネットファクシミリ装置に送信する工程と、を具備するようにしたものである。

【0032】

以下、本発明の実施の形態について図面を参照して詳細に説明する。

【0033】

(実施の形態1)

図1は、本発明の実施の形態1に係る通信制御装置が動作するネットワークを示す概念図である。本実施の形態の通信制御装置100は、IFAX101に接続され、IFAX101とそれに接続されたネットワークとの間で電子メール通信を行う場合に、その通信プロトコルを変換するアダプタとして機能するため、本実施の形態においては、以下、単にアダプタ(ADPT)と呼ぶこととする。

【0034】

このようなIFAX101に接続されたADPT100は、PC等の通信端末102と共に、LAN(Local Area Network)等のネットワーク103に接続されている。このネットワーク103は、グループウェアソフトを利用したサーバ(以下、「グループウェアサーバ」という)104により管理されている。以下において、このグループウェアサーバ104に管理されるネットワーク103をグループウェアネットワーク103と呼ぶこととする。

【0035】

このグループウェアサーバ104は、例えば、LOTUS社(米国)のNOTES等のグループウェアソフトを採用し社内ネットワークを構築する。これにより、PC102等のクライアント端末は、グループウェアネットワーク103で情報の共有を実現することができる。また、グループウェアサーバ104は、WEBサーバとしての機能を有し、グループウェアネットワーク103に接続されたPC102等のクライアント端末、あるいは、外部のクライアント端末は、W

WWブラウザを利用することでグループウェアネットワーク103における情報の共有を実現することができる。本実施の形態に係る発明は、グループウェアサーバ104がWEBサーバとして機能する場合に顕著な効果を奏するため、特にこの場合について説明する。

【0036】

このグループウェアネットワーク103の外部にあるLAN105に接続されたPC106が電子メールをグループウェアネットワーク103上のPC102等のクライアント端末に送信する場合、PC106等から送信された電子メールは、LAN105を介してメールサーバ107に送信される。そして、メールサーバ107で送信先等が判断され、インターネット108を介してグループウェアサーバ104に転送される。

【0037】

グループウェアサーバ104は、外部からの電子メールを受信すると、そのアドレス情報からユーザ名を判断する。そして、ユーザ名に対応するクライアントがグループウェアネットワーク103上に存在するか判断し、存在する場合には、そのユーザ名に対応するメールボックスに受信した電子メールデータを格納する。そして、そのユーザ名に対応するクライアント端末からアクセスがあった場合、その受信した電子メールをWWWブラウザ上で表示できるように電子メールデータの変換処理を行う。これにより、PC102等のクライアント端末は、WWWブラウザ上で電子メールを見ることができる。

【0038】

図2は、このような場合におけるグループウェアサーバ104及びグループウェアネットワーク103上のPC102等のクライアント端末周辺における通信プロトコルを説明するための概念図である。

【0039】

LAN105に接続されたPC106からグループウェアネットワーク103上のPC102に電子メールを送信する場合、インターネット108を介して電子メールは、SMTPプロトコルに従ってグループウェアサーバ104に送信される。この電子メールは、グループウェアサーバ104において一時的に保持さ

れる。そして、PC102から要求があった場合にグループウェアサーバ104は、その電子メールのプロトコルをSMTPプロトコルからHTTPプロトコルに変換することでPC102のWWWブラウザ上で見るができるようにしている。

【0040】

なお、図2において、ファイアウォール(FIRE WALL)は、インターネット108とグループウェアネットワーク103との間に配設され、インターネット108からのデータの流入を防止し、グループウェアネットワーク103上のクライアント端末からの要求に応答するデータだけグループウェアネットワーク103内に受け入れる機能を有するものである。

【0041】

これに対して、LAN105に接続されたIFAX109が電子メールをグループウェアネットワーク103上のIFAX101に送信する場合、PC106からの電子メールと同様に、IFAX109からメールサーバ107、インターネット108を介してグループウェアサーバ104に転送される。そして、グループウェアサーバ104でユーザ名が判断され、そのユーザ名に対応するクライアントが存在する場合には、そのユーザ名に対応したメールボックスに受信した電子メールデータが格納される。さらに、そのユーザ名に対応するIFAX101からADPT100を介してアクセスがあった場合、PC106からの電子メールと同様に、その受信した電子メールデータの変換処理を行う。

【0042】

図2を用いて説明すると、LAN105に接続されたIFAX109からグループウェアネットワーク103上のIFAX101に電子メールを送信する場合、上述のPC106からの電子メールと同様に、インターネット108を介して電子メールは、SMTPプロトコルに従ってグループウェアサーバ104に送信される。この電子メールは、グループウェアサーバ104において一時的に保持される。そして、IFAX101からADPT100を介して要求があった場合にグループウェアサーバ104は、その電子メールのプロトコルをSMTPプロトコルからHTTPプロトコルに変換するようにしている。

【0043】

ADPT100は、このHTTPプロトコルに従って処理された電子メールデータを受け取り、IFAX101との間でさらにプロトコルの変換処理を行う。すなわち、ADPT100は、IFAX101の動作可能なプロトコルであるPOP3（送信時には、SMTP）に従って電子メールデータをIFAX101に受け渡す。これにより、IFAX101は、通常の電子メールの通信処理と同様に、電子メールの受信を行うことができ、受信したその電子メールの印刷を行うことができる。

【0044】

図3は、上述のような機能を有する本ADPT100のハードウェア構成を示すブロック図である。

【0045】

中央処理部（CPU）200は、各種プログラムを実行してADPT100の各部を制御する。ROM201は、CPU200が実行するプログラムを格納する。RAM202は、プログラムのデータ領域として使用されると共に、所定のデータを格納するメモリとして使用される。

【0046】

第1LANインタフェース（以下、「第1LANI/F」という）203は、グループウェアネットワーク103との間のデータの送受信を制御するインタフェースである。第2LANインタフェース（以下、「第2LANI/F」という）204は、IFAX101との間のデータの送受信を制御するインタフェースである。なお、第2LANI/F204は、既存の全てのIFAX101が備えるインタフェースと接続されるため、各機種仕様等に限定されことなく既存のIFAX101の全ての機種に接続することができる。これら2つのLANI/Fにより本ADPT100は、IFAX100とグループウェアネットワーク103との間で動作する。

【0047】

バス205は、CPU200、ROM201、RAM202、第1LANI/F203及び第2LANI/F204間でデータが転送される経路である。

【0048】

図4は、上記実施の形態に係るADPT100の主要な機能を示すブロック図である。

【0049】

信号種別判定部400は、第2LANI/F204を介してIFAX101から出力されるコマンド信号の種別を判定する。そして、コマンド信号の種別に応じて、SMTP・POP3処理部401、HTTP処理部402及び電子メール通信部403にそのコマンド信号を受信した旨の通知をする。

【0050】

SMTP・POP3処理部401は、信号種別判定部400から通知を受けると、第2LANI/F204を介してIFAX101との間でSMTPプロトコル又はPOP3プロトコルに従って各種信号の通信を行う。

【0051】

HTTP処理部402は、信号種別判定部400から通知を受けると、第1LANI/F203を介してグループウェアネットワーク103との間でHTTPプロトコルに従って、各種信号の通信を行う。

【0052】

電子メール通信部403は、信号種別判定部400から通知を受けると、第2LANI/F204を介してIFAX101との間で電子メールデータの通信を行う。IFAX101から電子メールを受信する場合、電子メール通信部403は、受信した電子メールデータをRAM202に格納する。一方、IFAX101に電子メールを送信する場合、電子メール通信部403は、RAM202に格納された電子メールデータを取り出し、送信する。

【0053】

HTML通信部404は、第1LANI/F203を介して、グループウェアネットワーク103との間でHTML文書データの通信を行う。

【0054】

HTML処理部405は、HTML通信部404が受信したHTML文書データに所定のデータの書き込みを行う一方、RAM202に格納された電子メール

データのHTML文書への変換処理を行う。

【0055】

次に、上記構成を有するADPT100が接続されたIFAX101からグループウェアサーバ104に電子メールを送信する場合の処理について、図5に示すシーケンス図を参照しながら、図6に示すフロー図を用いて説明する。図5は、本実施の形態に係るADPT100が接続されたIFAX101からグループウェアサーバ104に電子メールを送信する場合のシーケンス図を示す。図6は、本実施の形態に係るADPT100からグループウェアサーバ104に電子メールデータを送信する場合のフロー図を示す。

【0056】

グループウェアサーバ104に電子メールを送信する場合、まず、IFAX101は、ADPT100とのコネクション確立のための手順を実行する。すなわち、図5に示すように、IFAX101は、ADPT100に対して、まず、同期を取るためのコマンド信号(SYN)を送信する。そして、コマンド信号(SYN)に応答してADPT100から送信される、同期確認を示すコマンド信号(SYN ACK)を受信し、IFAX101は、このコマンド信号(SYN ACK)を受信したことを示すコマンド信号(ACK)を送信する。この手順を実行することにより、IFAX101とADPT100との間のコネクションが確立される。

【0057】

IFAX101とADPT100のコネクションが確立されると、ADPT100は、グループウェアサーバ104とのコネクション確立のための手順を実行する。ADPT100は、上述のIFAX101が実行したのと同じの手順を実行する。この手順を実行することにより、ADPT100とグループウェアサーバ104との間のコネクションが確立される。

【0058】

ADPT100とグループウェアサーバ104とのコネクションを確立する際に、最終確認となるコマンド信号(ACK)をグループウェアサーバ104に送信すると、ADPT100において、SMTP・POP3処理部401は、IF

A X 1 0 1 との間で S M T P プロトコルに従ってコマンド信号のやりとりを開始する。具体的には、まず、S M T P ・ P O P 3 処理部 4 0 1 は、受信 O K を示す応答信号 (2 2 0) を I F A X 1 0 1 に対して出力する。

【 0 0 5 9 】

この " 2 2 0 " を受信すると、I F A X 1 0 1 は、通信路の使用開始宣言を示すコマンド信号 (H E L O) を A D P T 1 0 0 に対して出力する。この " H E L O " を受信すると、A D P T 1 0 0 において、信号種別判定部 4 0 0 は、S M T P ・ P O P 3 処理部 4 0 1 にその旨を通知する。この通知を受けると、S M T P ・ P O P 3 処理部 4 0 1 は、受信 O K を示す応答信号 (2 5 0) を I F A X 1 0 1 に対して出力する。

【 0 0 6 0 】

そして、これ以降、I F A X 1 0 1 から出力されるメッセージの送信者名を示すコマンド信号 (M A I L) 、メッセージの宛先名を示すコマンド信号 (R C P T) 及びメッセージの送信開始を示すコマンド信号 (D A T A) を受信して、S M T P ・ P O P 3 処理部 4 0 1 は、各コマンド信号に対して、" 2 5 0 " 、" 2 5 0 " 及び " 3 5 4 " という応答信号を I F A X 1 0 1 に出力する。なお、この " 3 5 4 " は、グループウェアサーバ 1 0 4 から後述する送信フォームを受け取ってから I F A X 1 0 1 に出力される。

【 0 0 6 1 】

この " 3 5 4 " を受信した後、I F A X 1 0 1 から出力される電子メールデータ及び通信路の使用終了宣言を示すコマンド信号 (Q U I T) を受信する。そして、S M T P ・ P O P 3 処理部 4 0 1 は、電子メールデータの受信完了時には " 2 5 0 " 、" Q U I T " に対しては " 2 2 1 " という応答信号を I F A X 1 0 1 に出力する。これにより、I F A X 1 0 1 と A D P T 1 0 0 との間のコネクションが切断される。このように、I F A X 1 0 1 と A D P T 1 0 0 との間では、通常の電子メールデータのやりとりと同様に、S M T P プロトコルに従って各種信号や電子メールデータのやりとりが行われる。

【 0 0 6 2 】

なお、電子メールデータの受信完了時に出力する " 2 5 0 " は、グループウェア

アサーバ104から後述する”POST”の応答信号を受信してからIFAX101に出力される。

【0063】

一方、IFAX101から”HELO”を受信すると、ADPT100において、信号種別判定部400は、HTTP処理部402にその旨を通知する。この通知を受けると、HTTP処理部402は、グループウェアサーバ104との間でHTTPプロトコルに従ってコマンド信号のやりとりを開始する。具体的には、まず、HTTP処理部402は、接続を要求するコマンド信号(GET)をグループウェアサーバ104に対して出力する。これにより、HTTPプロトコルに従ってグループウェアサーバ104と接続される(ST601)。

【0064】

なお、ここでは、単にHTTPプロトコルに従って接続しているが、接続の際、SSL (Secure Socket Layer) 等の技術を用いてグループウェアサーバ104との間で交換されるデータのセキュリティを守るようにしても良い。

【0065】

この”GET”を受信すると、グループウェアサーバ104は、応答信号として、認証要求を含むエラー信号をADPT100に対して出力する。このエラー信号は、ヘッダとHTML文書データで構成され、そのHTML文書データに認証する方法が指定されている。これにより、グループウェアサーバ104から認証方法が指定される(ST602)。

【0066】

このエラー信号を受信すると、HTTP処理部402は、送信フォームの要求を示すコマンド信号(GET)に予め設定されているユーザID (UID) 及びパスワードを付与して送信する(ST603)。

【0067】

この”GET”を受信すると、グループウェアサーバ104は、その”GET”に付与されたUID及びパスワードが適正なものか判断し、適正である場合には送信フォームを含むデータ(以下、「送信フォームデータ」という)をADPT100に対して出力する(ST604)。

【0068】

図7は、グループウェアサーバ104から送信される送信フォームデータのソースデータを示している。図7に示すように、送信フォームデータは、ヘッダとHTML文書データで構成され、そのHTML文書データに送信フォームが含まれている。この送信フォームを受信することで、ADPT100は、図8に示す送信フォームを認識することができる。なお、図8は、グループウェアサーバ104から送信される送信フォームの概念図である。

【0069】

送信フォームデータを受信すると、ADPT100において、HTML通信部404は、この”DATA”からHTML文書データで記述された送信フォームを抽出し、送信フォームを取得する(ST605)。このとき、HTTP処理部402は、この送信フォームデータを受信した旨を信号種別判定部400に通知する。

【0070】

送信フォームデータを受信した旨の通知を受けると、信号種別判定部400は、SMTP・POP3処理部401にその旨を通知する。この通知を受けると、上述のように、ADPT100において、SMTP・POP3処理部401は、”354”という応答信号をIFAX101に送信し、IFAX101からの電子メールデータの送信を促す。そして、IFAX101から送信された電子メールデータを電子メール通信部403が受信し、RAM202に格納する(ST606)。

【0071】

HTML処理部405は、RAM202に格納された電子メールデータから送信先(図8に示す「To」)、件名(図8に示す「Subject」)、ファイル名(図8に示す「File Name」)を抽出し、受信した送信フォームの所定位置に書き込む。そして、この送信フォームをHTML通信部404に渡す。HTML通信部404は、この送信フォームを含むコマンド信号(POST)をグループウェアサーバ104に送信すると共に電子メールデータをグループウェアサーバ104に送信する(ST607)。

【0072】

図9は、ADPT100が送信する”POST”のソースデータを示している。図9に示すように、”POST”は、ヘッダと送信データで構成され、その送信データに上述の送信フォームに書き込まれる所定情報が含まれている。具体的には、図9に示すように、送信先（a b c @ d e f . c o m）、件名（t e s t）及びファイル名（¥¥ i m a g e . t i f）が記述されている。この”POST”を受信することで、グループウェアサーバ104は、図10に示す所定情報が書き込まれた送信フォームを認識することができる。なお、図10は、ADPT100から送信される送信データが記述された送信フォームの概念図である。

【0073】

このような”POST”及び電子メールデータを受信すると（ST608）、送信フォームに記述された情報に従って、グループウェアサーバ104は、CGI処理を起動し（ST609）、送信フォームに記述された送信先の電子メールアドレスの検証を行う（ST610）。具体的には、その送信先の電子メールアドレスがグループウェアネットワーク103上のクライアント端末かどうかを判定する。ここで、グループウェアネットワーク103上のクライアント端末である場合には、電子メールデータは、該当するメールボックスに格納される（ST611）。一方、グループウェアネットワーク103上のクライアント端末でない場合には、電子メールデータは、インターネット108を介して他のメールサーバに転送される（ST612）。

【0074】

その後、グループウェアサーバ104は、電子メールデータの受信処理の終了を示すため、”POST”の応答信号をADPT100に出力する。これにより、グループウェアサーバ104とADPT100との間のコネクションが切断される。このように、グループウェアサーバ104とADPT100の間では、IFAX101からの”HELO”の受信をきっかけにして、HTTPプロトコルに従って各種信号や電子メールデータのやりとりが行われる。

【0075】

このように本実施の形態のADPT100によれば、IFAX101からグル

ープウェアサーバ104に電子メールを送信する際、IFAX101との間でSMTPプロトコルに従って各種信号や電子メールデータの通信を行う一方、グループウェアサーバ104との間でHTTPプロトコルに従って各種信号や電子メールデータの通信を行う。このため、HTTPプロトコルに従って通信が行われるグループウェアネットワーク103においても、IFAX101は、正常に電子メールの送信動作を行うことができる。

【0076】

また、本実施のADPT100によれば、グループウェアサーバ104から送信フォームデータを受信した後、IFAX101に対して”354”を送信する。そして、IFAX101から電子メールデータを受信した後、送信先等の情報を記述して送信フォームをグループウェアサーバ104に送信する。このため、送信フォームを認識する前に電子メールデータがIFAX101から送信され、電子メールデータの受信から長時間が経過することによるADPT100での誤動作を防止することができる。これにより、確実に電子メールの送信動作を行うことができる。

【0077】

次に、ADPT100が接続されたIFAX101がグループウェアサーバ104から電子メールを受信する場合の処理について、図11に示すシーケンス図を参照しながら、図12に示すフロー図を用いて説明する。図11は、本実施の形態に係るADPT100が接続されたIFAX101がグループウェアサーバ104から電子メールを受信する場合のシーケンス図を示す。図12は、本実施の形態に係るADPT100がグループウェアサーバ104から電子メールデータを受信する場合のフロー図を示す。

【0078】

グループウェアサーバ104から電子メールを受信する場合においても、グループウェアサーバ104に電子メールを送信する場合と同様に、IFAX101は、まず、ADPT100とのコネクション確立のための手順を実行する。また、IFAX101とADPT100のコネクションが確立されると、ADPT100も、グループウェアサーバ104に電子メールを送信する場合と同様に、グ

グループウェアサーバ104とのコネクション確立のための手順を実行する。

【0079】

ADPT100とグループウェアサーバ104とのコネクションを確立する際に、最終確認となるコマンド信号（ACK）をグループウェアサーバ104に送信すると、ADPT100において、SMTP・POP3処理部401は、IFAX101との間でPOP3プロトコルに従ってコマンド信号のやりとりを開始する。具体的には、まず、SMTP・POP3処理部401は、肯定応答を示すOKレスポンスをIFAX101に対して出力する。

【0080】

このOKレスポンスを受信すると、IFAX101は、メールボックス名の送信を示すコマンド信号（USER）をADPT100に対して出力する。この“USER”を受信すると、ADPT100において、信号種別判定部400は、SMTP・POP3処理部401にその旨を通知する。この通知を受けると、SMTP・POP3処理部401は、肯定応答を示すOKレスポンスをIFAX101に対して出力する。

【0081】

そして、これ以降、SMTP・POP3処理部401は、IFAX101から出力されるメールボックス・パスワードの送信を示すコマンド信号（PASS）、受信状態の問い合わせを示すコマンド信号（STAT）、メールのダウンロード要求を示すコマンド信号（RETR）を受信して、各コマンド信号に対して、肯定応答として、OKレスポンスをIFAX101に出力する。

【0082】

なお、“STAT”を受信した後、IFAX101に出力するOKレスポンスには、受信する電子メールデータの数及び各電子メールデータの容量が含まれる。また、IFAX101から受信した“RETR”とこれに対する肯定応答としてIFAX101に出力するOKレスポンスの間に、ADPT100は、リンク先情報を含むコマンド信号（GET）をグループウェアサーバ104に送信すると共に、グループウェアサーバ104から送信される電子メールデータを受信する。

【0083】

そして、"RETR"に対する肯定応答として、OKレスポンスをIFAX101に出力した後、ADPT100は、電子メールデータをIFAX101に出力する。

【0084】

一方、IFAX101から"USER"を受信すると、ADPT100において、信号種別判定部400は、HTTP処理部402にその旨を通知する。この通知を受けると、HTTP処理部402は、グループウェアサーバ104との間でHTTPプロトコルに従ってコマンド信号のやりとりを開始する。具体的には、まず、HTTP処理部402は、接続を要求するコマンド信号(GET)をグループウェアサーバ104に対して出力する。これにより、HTTPプロトコルに従ってグループウェアサーバ104と接続される(ST1201)。

【0085】

この"GET"を受信すると、グループウェアサーバ104は、応答信号として、認証要求を含むエラー信号をADPT100に対して出力する。このエラー信号は、ヘッダとHTML文書データで構成され、そのHTML文書データに認証する方法が指定されている。これにより、グループウェアサーバ104から認証方法が指定される(ST1202)。

【0086】

このエラー信号を受信すると、HTTP処理部402は、受信フォームの要求を示すコマンド信号(GET)に予め設定されているユーザID(UID)及びパスワードを付与して送信する(ST1203)。

【0087】

この"GET"を受信すると、グループウェアサーバ104は、その"GET"に付与されたUID及びパスワードが適正なものか判断し、適正である場合に応答信号として、受信フォームを含むデータ(以下、「受信フォームデータ」という)をADPT100に対して出力する(ST1204)。

【0088】

図13は、グループウェアサーバ104から送信される受信フォームデータの

ソースデータを示している。図13に示すように、受信フォームデータは、ヘッダとHTML文書データで構成され、そのHTML文書データに受信フォームが含まれている。この受信フォームを受信することで、ADPT100は、例えば、図14に示す受信フォームを認識することができる。なお、図14は、グループウェアサーバ104から送信される受信フォームの概念図である。

【0089】

受信フォームデータを受信すると、ADPT100において、HTML通信部404は、この受信フォームデータからHTML文書データで記述された受信フォームを抽出し、受信フォームを取得する(ST1205)。このとき、HTTP処理部402は、この受信フォームデータを受信した旨を信号種別判定部400に通知する。

【0090】

受信フォームデータを受信した旨の通知を受けると、信号種別判定部400は、SMTP・POP3処理部401にその旨を通知する。この通知を受けると、SMTP・POP3処理部401は、HTML文書データで記述された受信フォームの中からHTML処理部405が抽出した電子メールデータの数及び各電子メールデータの容量を”STAT”に対するOKレスポンスに付与して、IFAX101に送信する。

【0091】

受信フォームを取得すると、ADPT100において、その受信フォームから新規の電子メールデータの有無が判断される(ST1206)。ここで、新規の電子メールデータがない場合には、IFAX101における電子メールの受信処理が終了する(ST1207)。

【0092】

一方、新規の電子メールデータがある場合には、その受信データを指定した受信フォーム、言い換えると、リンク先が指定された受信フォームを含むコマンド信号(GET)をグループウェアサーバ104に送信する(ST1208)。ここでは新規の電子メールデータがあるものとする。

【0093】

図15は、ADPT100が送信する受信フォームを含む”GET”のソースデータを示している。図15に示す受信フォームを含む”GET”を受信することで、グループウェアサーバ104は、図14に示す上側の電子メールデータの受信要求を認識することができる。

【0094】

このような”GET”を受信すると(ST1209)、グループウェアサーバ104は、その”GET”に対応する電子メールデータをADPT100に対して送信する(ST1210)。

【0095】

このとき、グループウェアサーバ104から送信される電子メールデータは、HTML文書データで記述されている。HTML通信部404は、この電子メールデータを受信する(ST1211)。そして、HTML処理部405は、このHTML文書で記述された電子メールデータからTIFFファイルを抽出し(ST1212)、RAM202にそのTIFFファイルを格納する。

【0096】

RAM202にTIFFファイルが格納されると、電子メール通信部403は、そのTIFFファイルを取り出して、IFAX101に転送する(ST1213)。

【0097】

そして、電子メールデータを転送した後、図11に示すように、IFAX101から出力される電子メールの削除要求を示すコマンド信号(DELE)を受信する。この”DELE”を受信すると、受信フォームに記述された電子メールのうち、既にダウンロードした電子メールデータの削除を要求する受信フォームを含むコマンド信号(POST)をグループウェアサーバ104に出力する。ここでは、図14に示す上側の電子メールデータのダウンロードを終了しているため、この電子メールデータの削除を要求する。

【0098】

図16は、ADPT100が出力する受信フォームを含む”POST”のソースデータを示している。図16に示すように、この”POST”は、ヘッダと送

信データとで構成される。ヘッダには、削除を要求する電子メールデータを識別するための情報が含まれており、送信データには、図14の概念図で示した削除チェックボックスにチェックを入れるためのデータが含まれている。

【0099】

このような”POST”を受信すると、グループウェアサーバ104は、指定された電子メールデータを削除するためのCGI処理を起動し、その電子メールデータの削除処理を行う。そして、指定された電子メールデータの削除処理を行った後、グループウェアサーバ104は、削除処理を行った後に残った電子メールデータを含む受信フォームを再度、ADPT100に送信する。ここでは、図14に示す下側の電子メール情報だけが含まれる受信フォームがADPT100に送信される。

【0100】

この受信フォームを受信した後、ADPT100は、上述の”DELETE”に対する肯定応答として、OKレスポンスを出力する。そして、このOKレスポンスを受信したIFAX101は、上述した要領で、”RETR”をADPT100に出力することで、次の電子メールデータのダウンロード要求をする。ここでは、図14に示す下側の電子メールデータのダウンロードが要求されることとなるが、上述の説明と同様の処理であるため、説明を省略する。

【0101】

そして、受信フォームに含まれる全ての電子メールデータのダウンロードを終了後、”DELETE”をADPT100に出力し、ADPT100からこの肯定応答としてOKレスポンスを受信すると、IFAX101は、完了通知を示すコマンド信号(QUIT)を送信する。

【0102】

ADPT100は、この”QUIT”を受信し、これに対する肯定応答としてOKレスポンスを出力する。これにより、IFAX101とADPT100との間のコネクションが切断される。

【0103】

このように、IFAX101とADPT100の間では、通常の電子メール

データのやりとりと同様に、POP3プロトコルに従って各種信号や電子メールデータのやりとりが行われる。一方、ADPT100とグループウェアサーバ104との間では、IFAX101からの”USER”の受信をきっかけとしてHTTPプロトコルに従って各種信号や電子メールデータのやりとりが行われる。

【0104】

このように本実施の形態のADPT100によれば、IFAX101がグループウェアサーバ104から電子メールを受信する際、IFAX101との間でPOP3プロトコルに従って各種信号や電子メールデータの通信を行う一方、グループウェアサーバ104との間でHTTPプロトコルに従って各種信号や電子メールデータの通信を行う。このため、HTTPプロトコルに従って通信が行われるグループウェアネットワーク103においても、IFAX101は、正常に電子メールの受信動作を行うことができる。

【0105】

（実施の形態2）

図17は、本発明の実施の形態2に係るADPT100のハードウェア構成を示すブロック図である。図17において、図3と同一の符号が付されている構成については、同一の機能を有するものとし説明を省略する。

【0106】

図17に示すように、実施の形態2に係るADPT100は、実施の形態1に係るADPT100の構成に加え、所定のICカード1701に所定データの書込み、あるいは、ICカード1701に書き込まれたデータの読取りを行うICカードREAD/WRITE部（以下、「ICカードR/W部」という）1702を具備する。

【0107】

ICカード1701は、本ADPT100が接続されたIFAX101から電子メールの送受信を行うユーザに予め配布されているものである。なお、ICカード1701に書き込まれたデータの詳細については後述する。

【0108】

図18は、実施の形態2に係るADPT100の主要な機能を示すブロック図

である。なお、図18において、図4と同一の符号が付されている構成要素については、同一の機能を有するものとし説明を省略する。

【0109】

カード情報判定部1801は、ICカードスロット1702Aに装着されたICカード1701からICカードR/W部1702が読み取った情報の内容を判定する。そして、ICカード1701に署名処理又は署名暗号化処理に必要な情報が格納されている場合に署名暗号化処理部1802にその情報を与える。

【0110】

また、カード情報判定部1801は、ICカードR/W部1702が読み取った情報に基づいてICカード1701の装着の有無についても判定する。さらに、カード情報判定部1801は、ICカード1701に格納された電子メールアドレス情報を判定し、その電子メールアドレス情報を電子メール通信部403に通知する。

【0111】

署名暗号化処理部1802は、カード情報判定部1801から受け取った署名暗号化処理等に必要な情報に基づいて、電子メール通信部403がIFAX101から受信した電子メールデータに対して署名暗号化処理等の処理を行う。また、署名暗号化処理部1802は、カード情報判定部1801から受け取った署名暗号化処理等に必要な情報に基づいて、電子メール通信部403がグループウェアネットワーク103から受信した電子メールデータに施された署名暗号化処理等の解読処理を行う。

【0112】

ここで、ICカード1701に格納された情報について説明する。

【0113】

ICカード1701は、上述のように、IFAX101を用いて電子メール通信を行う各ユーザに配布されるものであり、各ユーザに付与された電子メールアドレス情報が格納されている。すなわち、ADPT100にICカード1701が装着されているときのみ、各ユーザは、自分の電子メールアドレスから電子メールを送信することができ、自分の電子メールアドレスに対する電子メールを受

信することができる。

【0114】

また、ICカード1701は、署名処理又は署名暗号化処理に必要となる情報を格納する。すなわち、ICカード1701は、自分の秘密鍵情報及び公開鍵情報を格納する。なお、送信先の公開鍵情報は、ADPT100のRAM202内に蓄積されている。

【0115】

次に、以上のような構成を有するADP100が接続されたIFAX101からグループウェアサーバ104に電子メールを送信する場合の処理について、図5に示すシーケンス図を参照しながら、図19に示すフロー図を用いて説明する。図19は、実施の形態2に係るADPT100がIFAX101から受信した電子メールデータに対する署名暗号化処理等の処理を示すフロー図である。なお、IFAX101から送信する電子メールデータには全て暗号化処理が施されるものとする。

【0116】

実施の形態2においても、IFAX101からグループウェアサーバ104に電子メールを送信する場合、実施の形態1で図5を用いて説明した場合と同様に、IFAX101とADPT100の間においてSMTPプロトコルに従って各種信号のやりとりが行われ、その後に電子メールデータを受信する。受信した電子メールデータは、以下に説明するように暗号化処理が施される一方、後述する送信フォームへの所定データの書込み処理が終了するまでオリジナルの電子メールデータがRAM202に保持される。

【0117】

IFAX101から電子メールデータを受信すると(ST1901)、カード情報判定部1801は、ICカードR/W部1702が読み取った情報に基づいて、ICカード1701がADPT100のスロット1702Aに挿入されているか判定する(ST1902)。

【0118】

ここで、ICカード1701がADPT100のスロット1702Aに挿入さ

れていない場合には、ADPT100では、通常の電子メールの送信処理が行われる（ST1903）。すなわち、IFAX101に付与された電子メールアドレスから電子メールの送信処理が行われる。

【0119】

一方、ICカード1701が本ADPT100のスロット1702Aに挿入されている場合には、ICカードR/W部1702は、ICカード1701からこのユーザに関する情報（以下、「ユーザ情報」という）を抽出する。このとき、このユーザの電子メールアドレス情報が抽出される（ST1904）。

【0120】

そして、カード情報判定部1801は、ICカードR/W部1702が抽出したユーザ情報から電子メールアドレス情報を判定し、電子メール通信部403に通知する。電子メール通信部403は、その電子メールアドレス情報を電子メールの送信元情報に設定する（ST1905）。具体的にいうと、抽出された電子メールアドレス情報が電子メールのヘッダ情報の[F r o m :]に設定される。

【0121】

電子メールの送信元情報が設定されると、本ADPT100において、S/MIME処理が施される。まず、本ADPT100において、送信先情報があるか判定される（ST1906）。具体的には、本ADPT100のRAM202に送信先の公開鍵情報が格納されているかが判定される。

【0122】

ここで、送信先情報がない場合には、カード情報判定部1801は、ICカードR/W部1702が抽出したユーザ情報から自己の秘密鍵情報を判定し、署名暗号化処理部1802に渡す。署名暗号化処理部1802は、この自己の秘密鍵情報を用いて署名処理を行う（ST1907）。

【0123】

具体的には、電子メールデータのメッセージデータからハッシュ関数等の不可逆性の関数で演算処理を行い、メッセージダイジェストを取り出し、そのメッセージダイジェストに自己の秘密鍵情報を用いて暗号化処理を施す。

【0124】

一方、送信先情報がある場合には、署名暗号化処理部1802は、この送信先の公開鍵情報を入手する。一方、カード情報判定部1801は、ICカードR/W部1702が抽出したユーザ情報から自己の秘密鍵情報を署名暗号化処理部1802に渡す。署名暗号化処理部1802は、この自己の秘密鍵情報及び送信先の公開鍵情報を用いて署名暗号化処理を行う（ST1908）。

【0125】

具体的には、まず、上述のように電子メールのメッセージからハッシュ関数等の不可逆性の関数で演算処理を行い、メッセージダイジェストを取り出し、そのメッセージダイジェストに自己の秘密鍵情報を用いて暗号化処理を施す。さらに、DEK（Data Encryption Key）と呼ばれる擬似乱数を用いた暗号鍵を生成する。そして、そのDEKに対して送信先の公開鍵情報を用いて暗号化処理を施す。一方、先に暗号化処理を施したメッセージダイジェスト（署名結果）及び電子メールのメッセージデータに対して、そのDEKで所定の暗号化方式（例えば、DES：Data Encryption Standard等）にしたがって暗号化処理を施す。

【0126】

そして、ST1907又はST1908で署名暗号化処理等を施した後、署名暗号化処理部1802は、その電子メールデータをRAM202に格納する（ST1909）。

【0127】

署名暗号化処理後の電子メールデータがRAM202に格納されると、図5で説明した場合と同様に、HTML処理部405は、RAM202に格納されたオリジナルの電子メールデータから送信先（図8に示す「To」）、件名（図8に示す「Subject」）、ファイル名（図8に示す「File Name」）を抽出し、受信した送信フォームの所定位置に書き込む。そして、この送信フォームをHTML通信部404に渡す。HTML通信部404は、この送信フォームを含むコマンド信号（POST）をグループウェアサーバ104に送信すると共に署名暗号化処理が施された電子メールデータをRAM202から取り出し、グループウェアサーバ104に送信する。このようにしてADPT100がIFAX101から受信した電子メールデータに対する署名暗号化等の処理を終了する。

【0128】

このように本実施の形態のADPT100によれば、IFAX101から電子メールデータを送信する際、HTTPプロトコルに従って通信が行われるグループウェアネットワーク103においても、IFAX101に正常に電子メールの送信動作を行わせることができるだけでなく、必要に応じてその電子メールデータに暗号化処理を施すことができるので、既存のIFAXに特別な構成を附加することなく、電子メールの秘匿性を確保することができる。

【0129】

また、電子メールに暗号化処理を施す際、本ADPT100は、各ユーザに配布されたICカード1701の有無を判定し、暗号化処理の可否を判断する。これにより、暗号化処理を行う必要がない電子メールデータは、暗号化処理を施すことなく送信できる一方、暗号化処理を行う必要がある電子メールデータは、暗号化処理を施して送信することができるので、簡単に暗号化処理の可否を判断することができる。

【0130】

さらに、電子メールに暗号化処理を施す際、本ADPT100は、挿入されたICカード1701内に格納された暗号化処理に必要な情報を用いて暗号化処理を施す。各ユーザが管理するICカード1701に格納された情報を用いて暗号化処理が行なわれるため、その情報の書き換え等を防止することができる。

【0131】

次に、本ADPT100が接続されたIFAX101がグループウェアサーバ104から電子メールを受信する場合の処理について、図11に示すシーケンス図を参照しながら、図20に示すフロー図を用いて説明する。図20は、ADPT100がグループウェアサーバ104から電子メールデータを受信し、その電子メールデータに施された署名暗号化処理等の解読を行うの処理を示すフロー図である。なお、図20において、図12と同一の符号については、同一の処理を行うものとする。また、グループウェアサーバ104から受信する電子メールは、全て暗号化処理が施されているものとする。

【0132】

実施の形態2においても、グループウェアサーバ104から電子メールデータを受信する場合、実施の形態1で図11を用いて説明した場合と同様に、IFAX101がまず、ADPT100とのコネクション確立のための手順を実行する。このとき、ADPT100は、このコネクション確立のために最初に送信される”SYN”を電子メールの受信指示として捉える。これにより、ADPT100において、この受信指示があるかが判定される(ST2001)。

【0133】

電子メールの受信指示があると判定されると、カード情報判定部1801は、ICカードR/W部1702が読み取った情報に基づいてICカード1701がADPT100のスロット1702Aに挿入されているか判定する(ST2002)。

【0134】

ここで、ICカード1701がADPT100のスロット1702Aに挿入されていない場合には、ADPT100では、IFAX101から指示したユーザの電子メールアドレス情報を確認することができないため、電子メールの受信処理は行われない(ST2003)。

【0135】

一方、ICカード1701がADPT100のスロット1702Aに挿入されている場合には、図11で説明したように、所定のコマンド信号及び応答信号が交換され、IFAX101とADPT100との間、ADPT100とグループウェアサーバ104との間のコネクションが確立される。そして、双方のコネクションが確立された後、図11で説明したのと同様の要領でADPT100は、HTTPプロトコルに従ってグループウェアサーバ104と接続する(ST1201)。

【0136】

HTTPプロトコルに従ってADPT100と接続後、グループウェアサーバ104から認証要求を含むエラー信号を受信すると、ADPT100において、HTTP処理部402は、予め設定されたUID及びパスワード受信フォームの要求を示すコマンド信号(GET)に付与して送信する(ST1203)。

【0137】

この”GET”を受信すると、ST1204において、所定の場合にグループウェアサーバ104から応答信号として出力される、受信フォームデータを受信する。そして、ADPT100において、HTML通信部404は、この受信フォームデータからHTML文書データで記述された受信フォームを抽出し、受信フォームを取得する（ST1205）。

【0138】

受信フォームを取得すると、ADPT100において、その受信フォームから新規の電子メールアドレスの有無が判断され（ST1206）、新規の電子メールアドレスがある場合、リンク先が指定された受信フォームを含むコマンド信号（GET）をグループウェアサーバ104に送信する（ST1208）。

【0139】

この”GET”を受信すると（ST1209）、ST1210においてグループウェアサーバ104から出力される、その”GET”に対応する、HTML文書データで記述された電子メールアドレスをHTML通信部404が受信する（ST1211）。そして、HTML処理部405は、このHTML文書で記述された電子メールアドレスからTIFFファイルを抽出し（ST1212）、RAM202にそのTIFFファイルを格納する。なお、このとき、TIFFファイルには暗号化処理が施されている。

【0140】

RAM202にTIFFファイルが格納されると、ADPT100において、送信者情報があるかが判定される（ST2004）。具体的には、ADPT100に送信者の公開鍵情報が格納されているかが判定される。なお、この公開鍵情報は、電子メールのメッセージダイジェストの暗号化を解読する際に用いられるものである。

【0141】

送信者の公開鍵情報がない場合には、その電子メールに付与された送信者の公開鍵情報をADPT100のRAM202に格納する（ST2005）。そして、署名暗号化処理部1802は、その電子メールアドレスが暗号化されているか判

定する（ST2006）。一方、送信者の公開鍵情報がある場合には、さらにその公開鍵情報を格納することなく、直接、その電子メールデータが暗号化されているか判定する（ST2006）。

【0142】

ここでは、電子メールデータが暗号化されているため、RAM202からそのTIFFファイルを取り出し、署名暗号化処理部1802は、そのTIFFファイルの復号化処理を行う（ST2007）。

【0143】

具体的には、暗号化されているDEKを自分の秘密鍵情報で復号化し、復号化したDEKで暗号化されたデータを復号化する。そして、復号化したデータから、電子メールデータをメッセージダイジェストとメッセージデータに分離する。その際、メッセージダイジェストを送信者の公開鍵情報で復号化し、その結果を保持しておく。一方、分離したメッセージデータから、上述したようなハッシュ関数を用いてメッセージダイジェストを抽出する。そして、そこで得たメッセージダイジェストと先ほど保持したメッセージダイジェストとを比較する。これにより、電子メールのメッセージデータが改ざんされていないか、また、正当な送信者から送信されたかを確認することができる。

【0144】

なお、メッセージデータが暗号化されていないような場合には、署名暗号化処理部1802は、そのメッセージダイジェストのみ復号化し、正当な送信者から送信されたかだけを確認する。

【0145】

そして、署名暗号化処理部1802は、このように復号化したTIFFファイルをRAM202に格納する（ST2008）。復号化処理後のTIFFファイルがRAM202に格納されると、図11で説明したのと同様に、電子メール通信部403は、そのTIFFファイルを取り出して、IFAX101に転送する（ST1213）。このようにしてADPT100がグループウェアサーバ104から受信した電子メールデータを復号化する処理が終了する。

【0146】

このように本実施の形態のADPT100によれば、グループウェアサーバ104から電子メールを受信する際、HTTPプロトコルに従って通信が行われるグループウェアネットワーク103においても、IFAX101に正常に電子メールの受信動作を行わせることができるだけでなく、その電子メールに暗号化処理が施されているか判断し、施されている場合にはその暗号化処理された電子メールデータを復号化し、IFAX101に転送する。このため、既存のIFAXに特別な構成を附加することなく、電子メールの秘匿性を確保して電子メールを受信することができる。

【0147】

また、電子メールの受信処理を行う際、ADPT100は、各ユーザに配布されたICカード1701の装着の有無を判定し、そのICカード1701がない場合には、電子メールの受信処理を行わない。このため、電子メールの受信の際に受信者の認証を行うことができる。したがって、単一のIFAX101を用いた場合でも、他の人に自分宛ての電子メールデータを見られるという事態を防止することができる。

【0148】

なお、本実施の形態では、ADPT100の挿入されるICカード1701は、署名暗号化に必要な情報等を格納するメモリカードのような構成を有している。しかし、ICカード1701の構成としては、これに限定されず、例えば、ICカード1701に署名暗号化処理のプログラム等を内蔵し、署名暗号化処理の一部又は全部をICカード1701内で行うようにしても良い。この場合には、例えば、本ADPT100から処理すべき、暗号化されたメッセージダイジェスト（ハッシュ値）又は暗号化されたDEKを受け取って所定の暗号化処理又は復号化処理の一部をICカード1701内で行うことができる。所定のデータを受け取って暗号化処理等の処理が行われるため、暗号化処理等の処理に必要な情報を単に格納する場合と比べて、暗号化処理等に必要な情報が他人により読み取られるのをより確実に防止することができる。

【0149】

また、本実施の形態では、ICカード1701に暗号化処理等に必要な情報を

格納し、その暗号化処理等の処理を行う暗号化処理装置100について説明している。しかし、これに限定されず、暗号化処理等に必要な情報は、暗号化処理装置100のメモリ等に格納しておいてももちろん良い。このように変更した場合にも、本実施の形態と同様の効果を得ることができる。

【0150】

【発明の効果】

以上説明したように本発明によれば、I F A Xとグループウェアサーバとの間で電子メール通信を行う際、I F A Xとの間でSMTPプロトコル又はPOP3プロトコルに従って各種信号や電子メールデータの通信を行う一方、グループウェアサーバとの間でHTTPプロトコルに従って各種信号や電子メールデータの通信を行うようにしたので、HTTPプロトコルで管理されたネットワーク上でもI F A Xを正常に動作させることができる。

【図面の簡単な説明】

【図1】

本発明の実施の形態1に係る通信制御装置（ADPT）が動作するネットワークを示す概念図

【図2】

実施の形態1に係るADPTの動作するグループウェアネットワーク上のクライアント端末周辺における通信プロトコルを説明するための概念図

【図3】

実施の形態1に係るADPTのハードウェア構成を示すブロック図

【図4】

実施の形態1に係るADPTの主要な機能を示すブロック図

【図5】

実施の形態1に係るADPTが接続されたI F A Xからグループウェアサーバに電子メールを送信する場合のシーケンス図

【図6】

実施の形態1に係るADPTからグループウェアサーバに電子メールデータを送信する場合のフロー図

【図 7】

実施の形態 1 に係る A D P T に対してグループウェアサーバから送信される送信フォームデータのソースデータを示す図

【図 8】

実施の形態 1 に係る A D P T に対してグループウェアサーバから送信される送信フォームの概念図

【図 9】

実施の形態 1 に係る A D P T が送信する” P O S T ” のソースデータを示す図

【図 1 0】

実施の形態 1 に係る A D P T から送信される送信データが記述された送信フォームの概念図

【図 1 1】

実施の形態 1 に係る A D P T が接続された I F A X がグループウェアサーバから電子メールを受信する場合のシーケンス図

【図 1 2】

実施の形態 1 に係る A D P T グループウェアサーバから電子メールデータを受信する場合のフロー図

【図 1 3】

実施の形態 1 に係る A D P T に対してグループウェアサーバから送信される受信フォームデータのソースデータを示す図

【図 1 4】

実施の形態 1 に係る A D P T に対してグループウェアサーバから送信される受信フォームの概念図

【図 1 5】

実施の形態 1 に係る A D P T が送信する受信フォームを含む” G E T ” のソースデータを示す図

【図 1 6】

実施の形態 1 に係る A D P T が出力する受信フォームを含む” P O S T ” のソースデータを示す図

【図17】

本発明の実施の形態2に係るADPTのハードウェア構成を示すブロック図

【図18】

実施の形態2に係るADPTの主要な機能を示すブロック図

【図19】

実施の形態2に係るADPTがIFAXから受信した電子メールデータに対する署名暗号化処理等の処理を示すフロー図

【図20】

実施の形態2に係るADPTがグループウェアサーバから電子メールデータを受信し、その電子メールデータに施された署名暗号化処理等の解読を行うの処理を示すフロー図

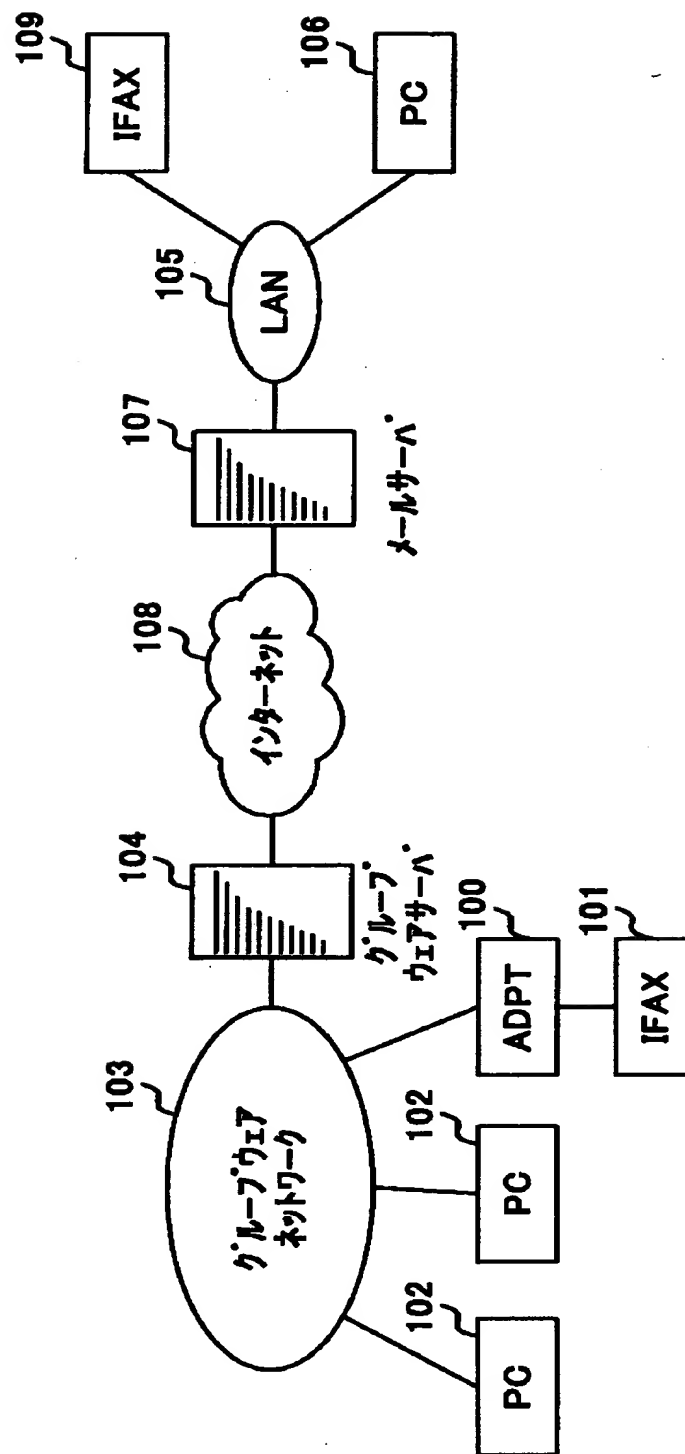
【符号の説明】

- 100 ADPT
- 101 IFAX
- 103 グループウェアネットワーク
- 104 グループウェアサーバ
- 203 第1LANI/F
- 204 第2LANI/F
- 400 信号種別判定部
- 401 SMTP・POP3処理部
- 402 HTTP処理部
- 403 電子メール通信部
- 404 HTML通信部
- 405 HTML処理部
- 1701 ICカード
- 1702 ICカードR/W部
- 1801 カード情報判定部
- 1802 署名暗号化処理部

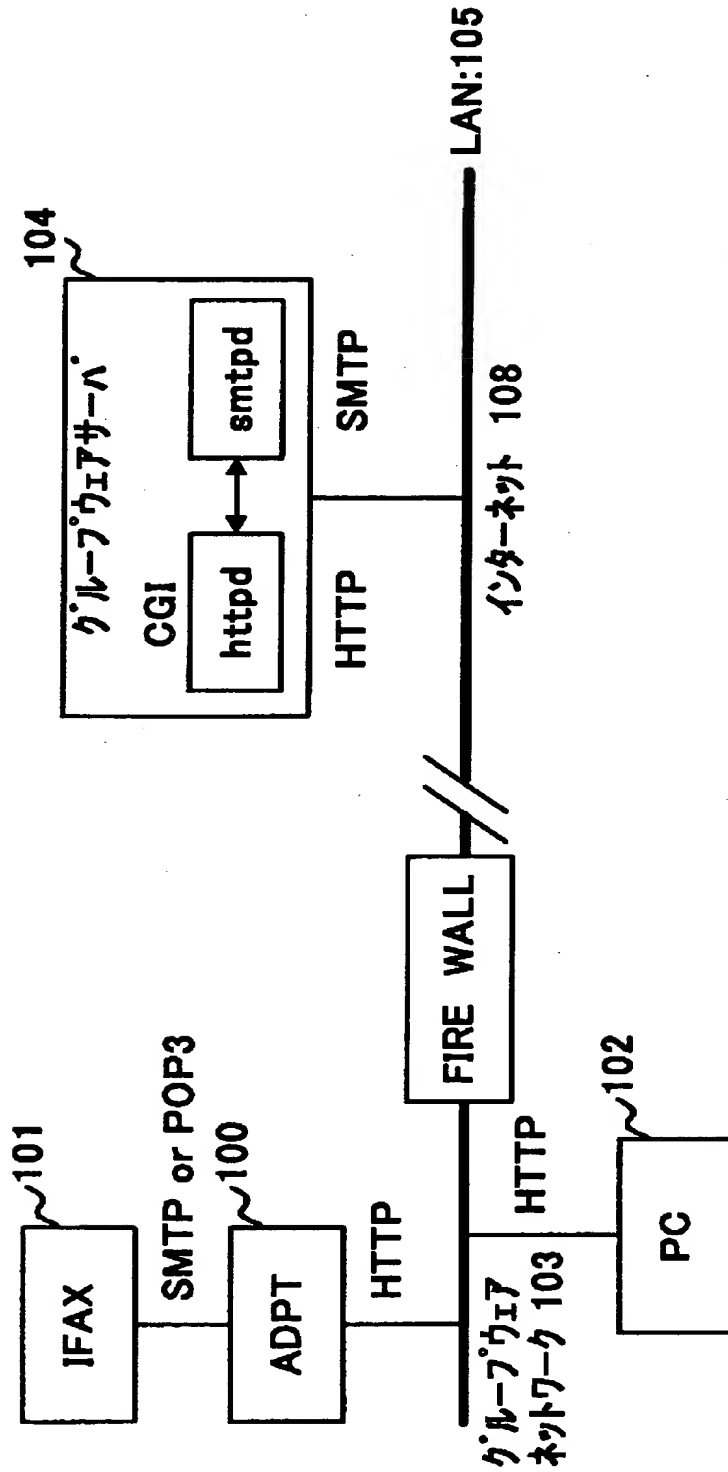
【書類名】

図面

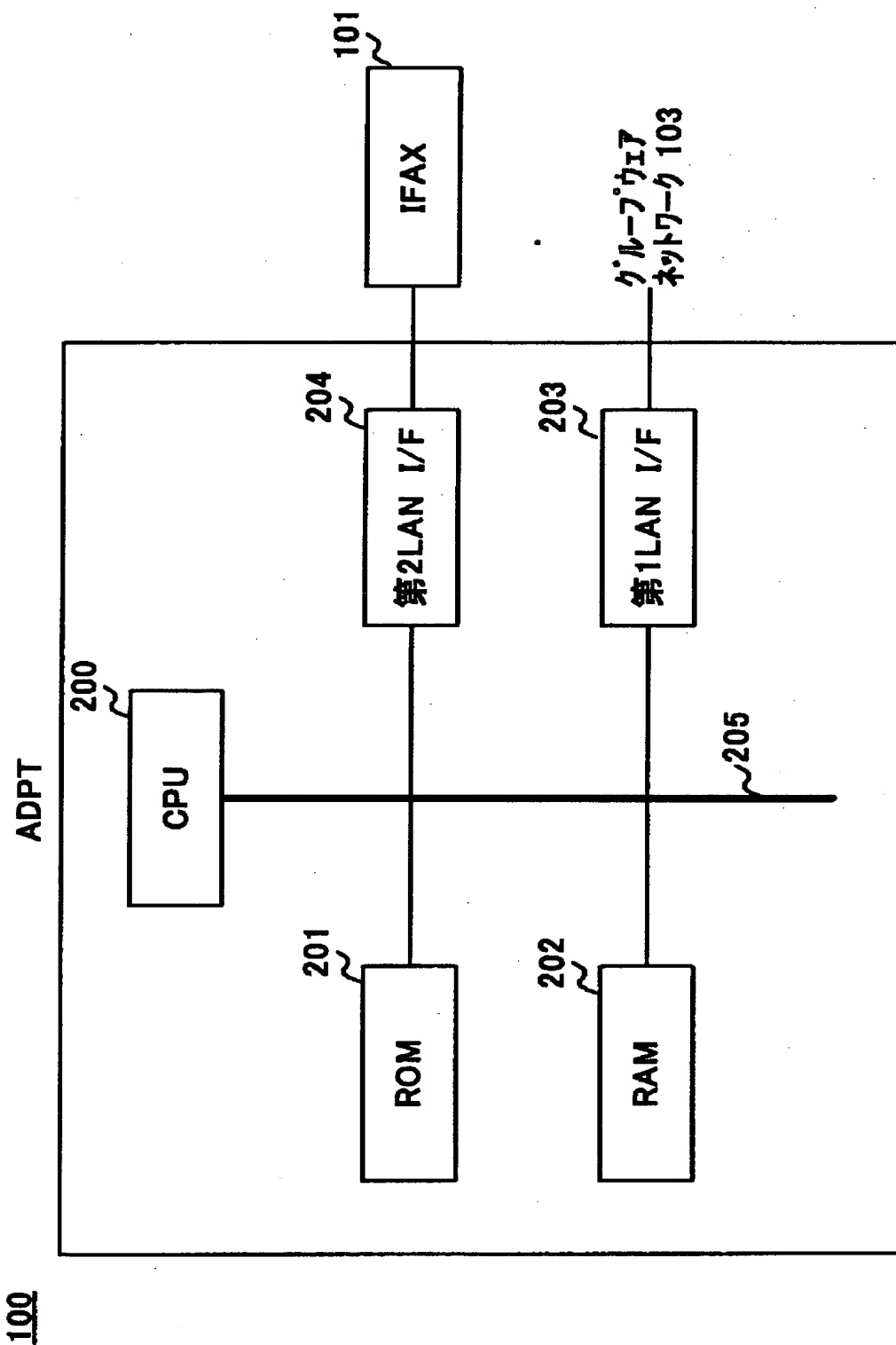
【図 1】



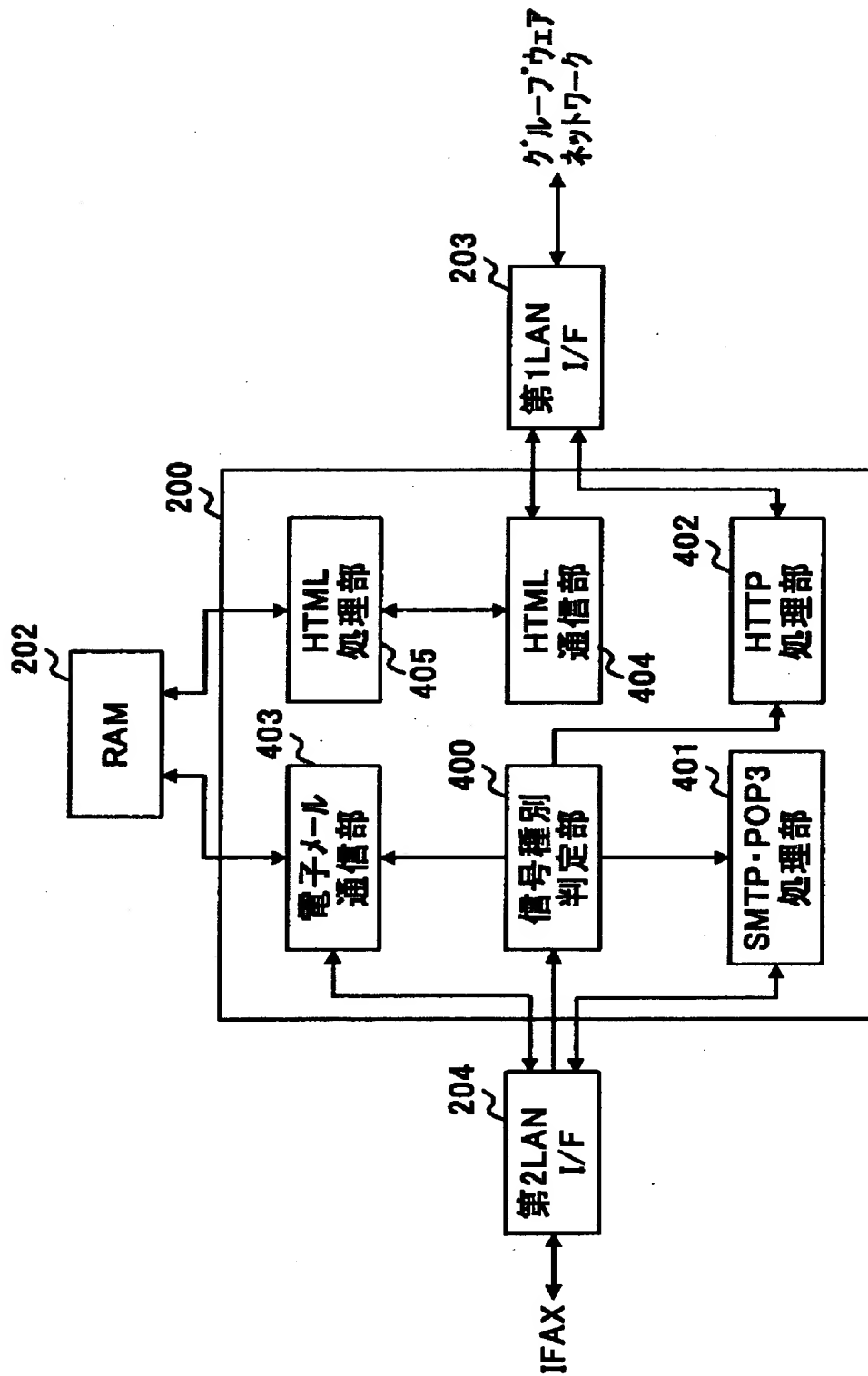
【図2】



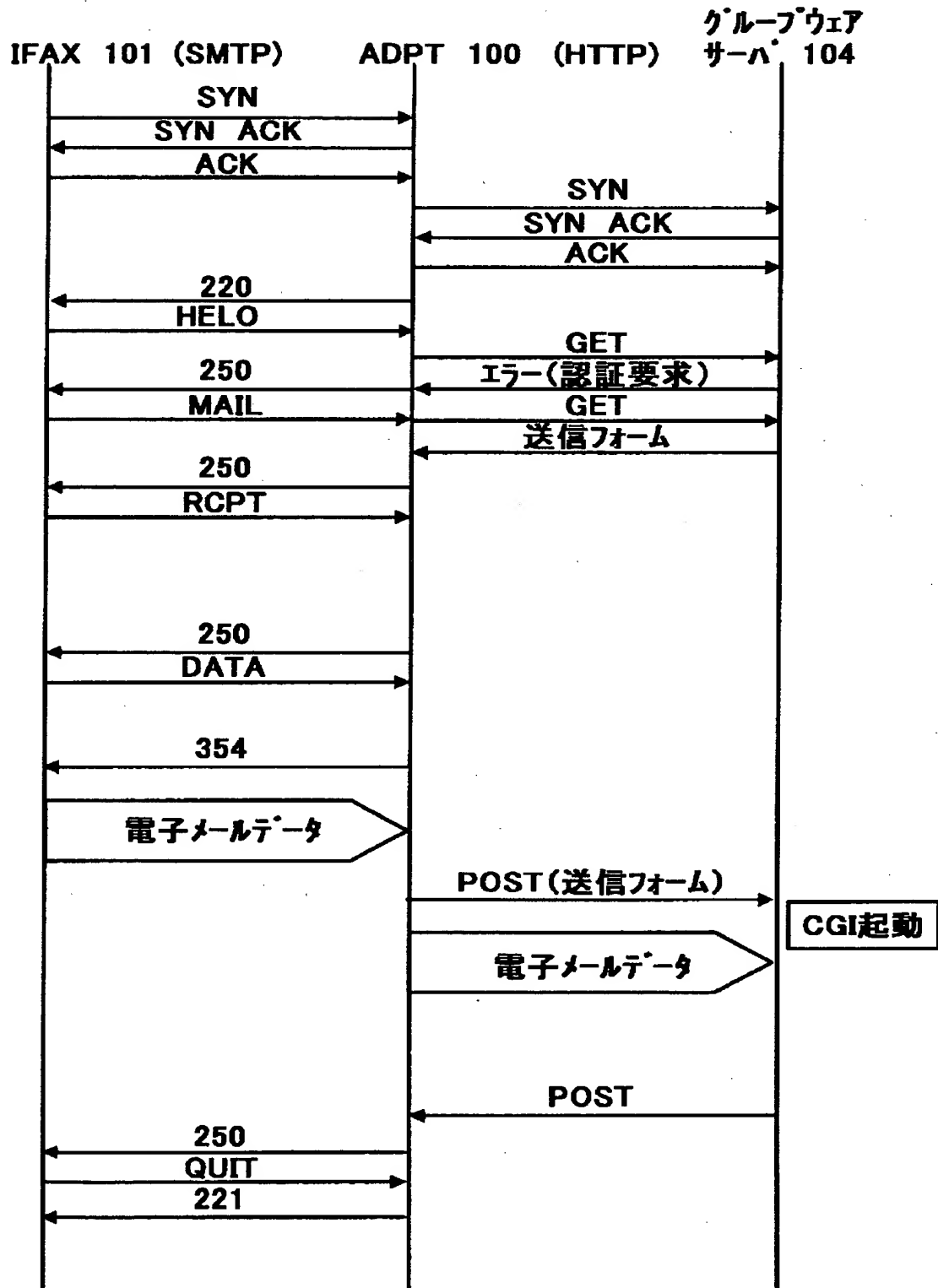
【図 3】



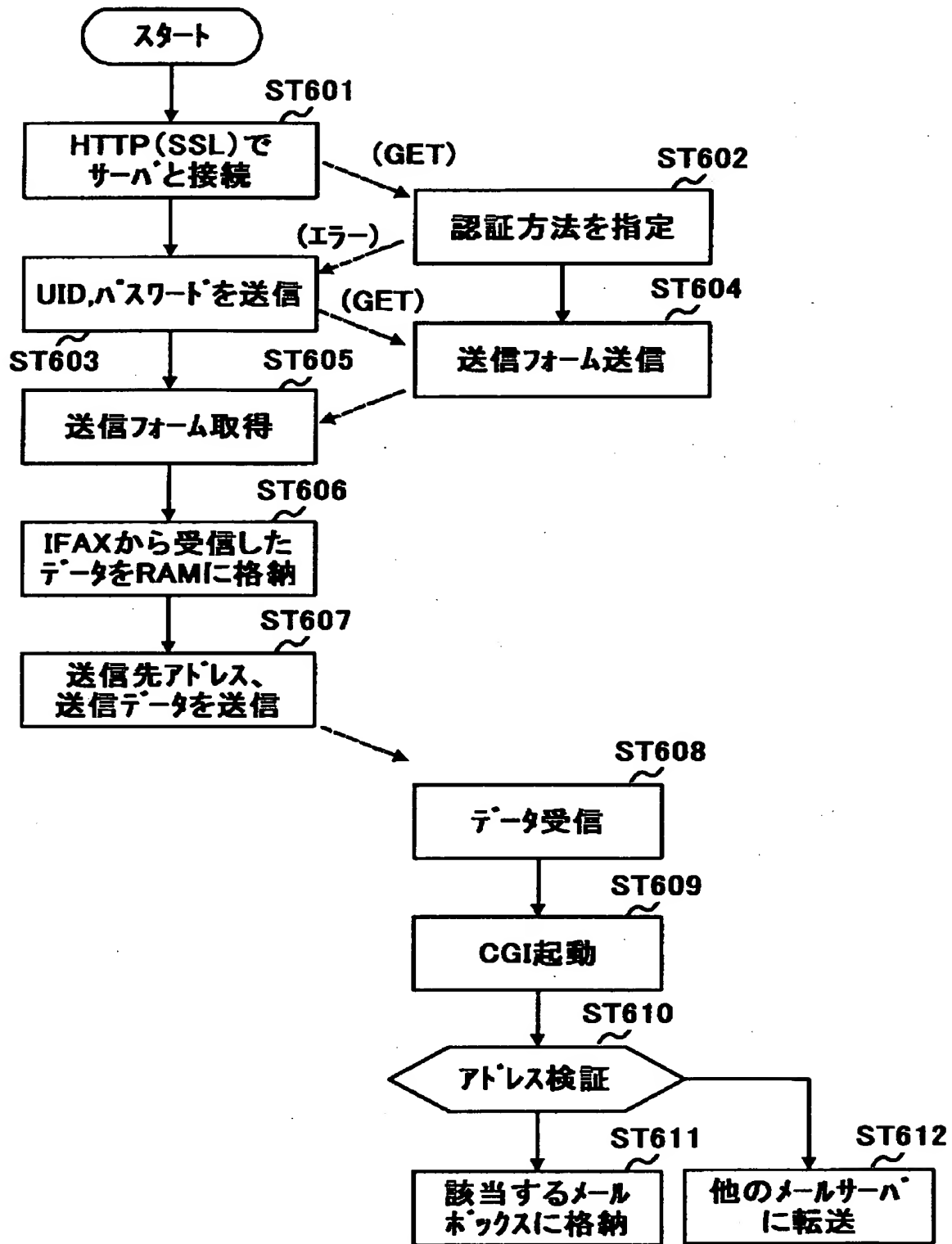
【図4】



【図 5】



【図6】



【図7】

HTTP/1.1 200 OK
Date: Fri, 23 Jun 2000 04:13:29 GMT
Server: hoge/1.0
Connection: close
Content-Type: text/html

```
<HTML>
<HEAD><TITLE>TX sample</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF">
<FORM ENCTYPE="multipart/form-data" ACTION="/upload.cgi" METHOD="post">
<TABLE>
<TR><TD ALIGN=right>TO: </TD>
<TD><INPUT TYPE="text" NAME="to" SIZE="60"></TD>
</TR>
<TR><TD ALIGN=right>Subject: </TD>
<TD><INPUT TYPE="text" NAME="subject" SIZE="60"></TD>
</TR>
<TR><TD ALIGN=right>File Name: </TD>
<TD><INPUT TYPE="file" NAME="file" SIZE="45"></TD>
</TR>
</TABLE>
<P><INPUT TYPE="submit" VALUE="SUBMIT">
</FORM>
</BODY>
</HTML>
```

ヘッダ

HTML
本文

【図 8】

TO : _____

Subject : _____

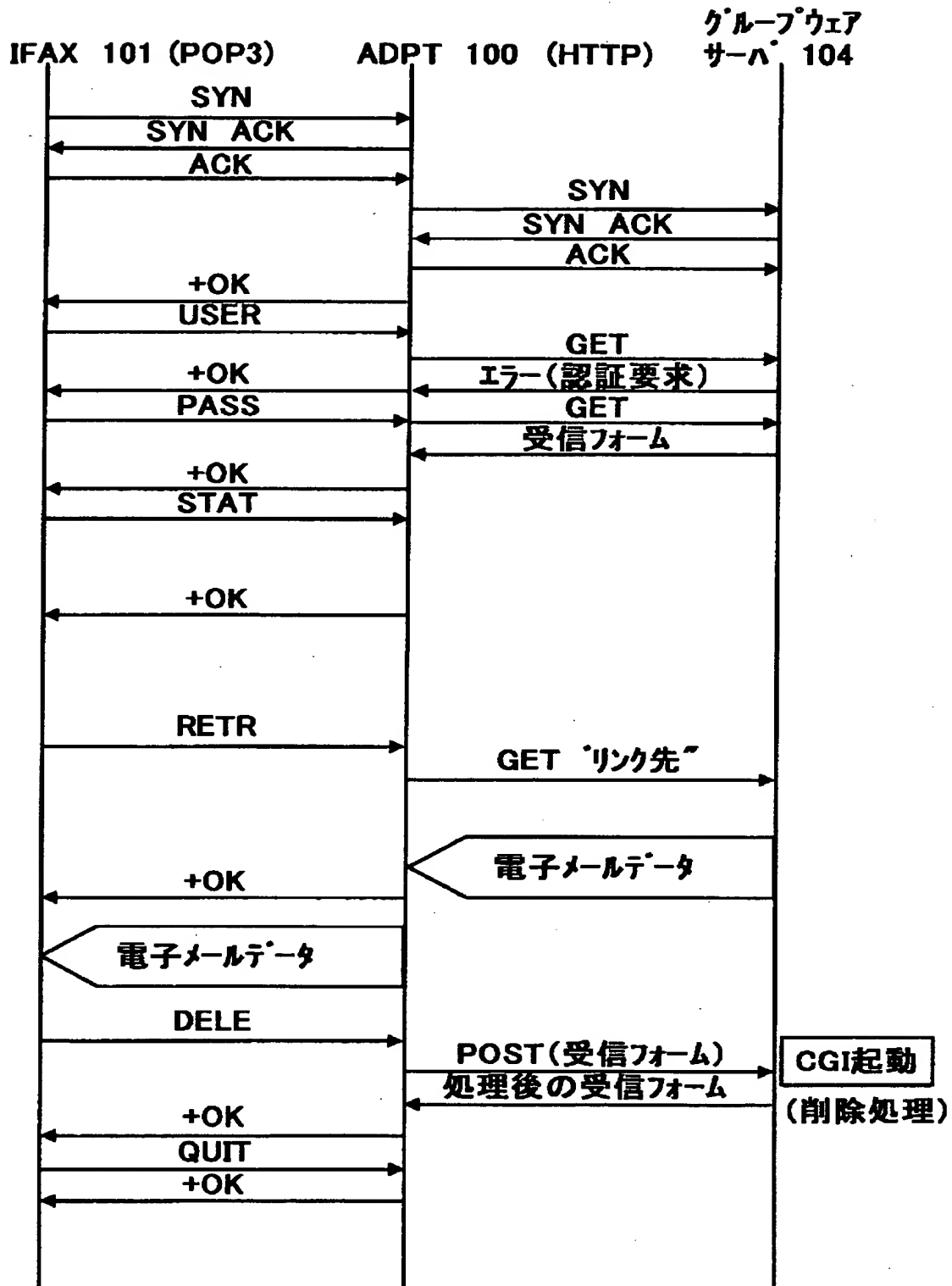
File Name : _____ 参照...

SUBMIT

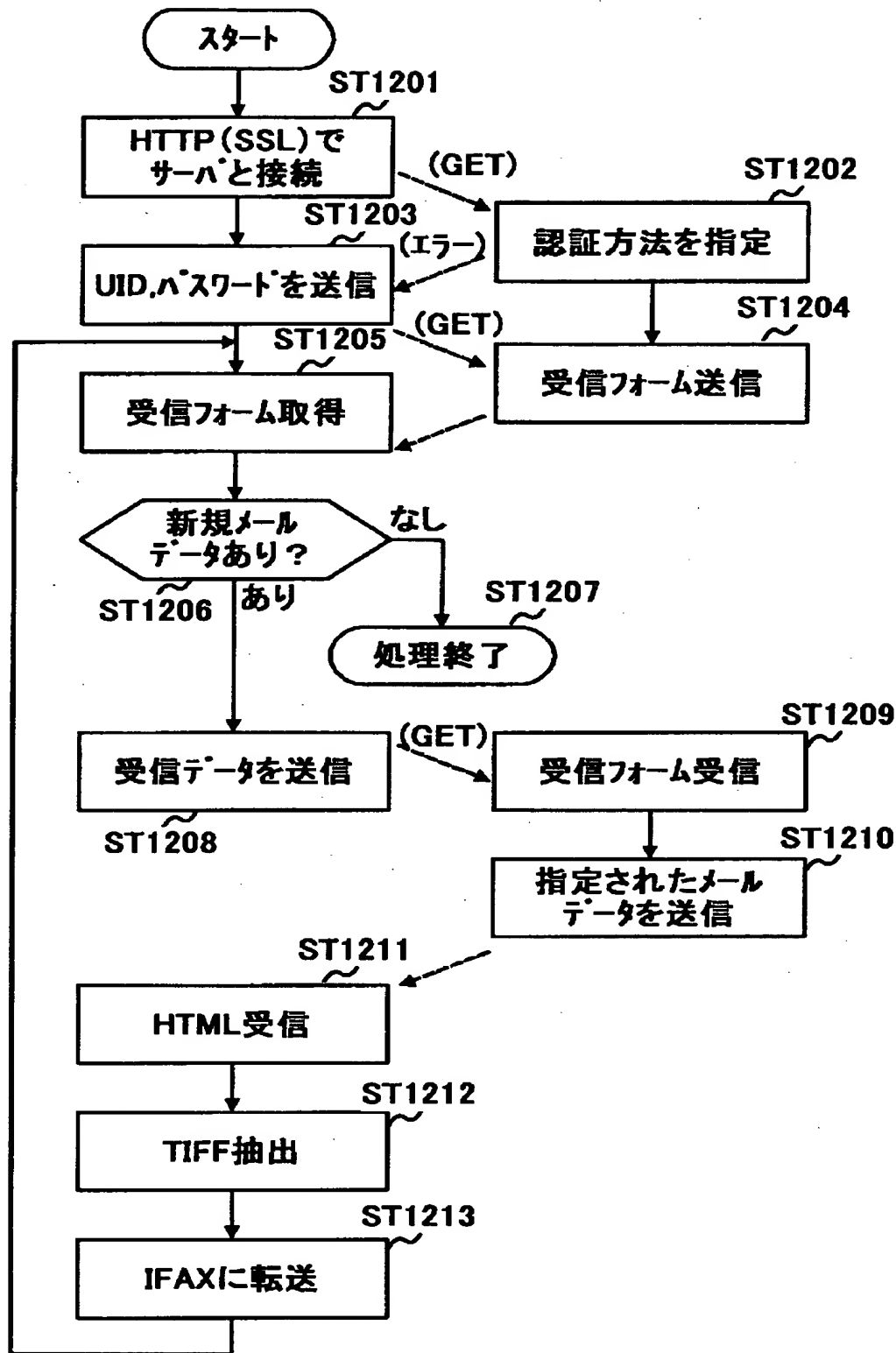
【図10】

TO :	abc@def.com		
Subject :	test		
File Name :	D : \image.tif	参照...	
<u>SUBMIT</u>			

【図 11】



【図12】



【図 13】

```

HTTP/1.1 200 OK
Date : Mon, 26 Jun 2000 05:06:04 GMT
Server : hoge/1.0
Connection : close
Content-Type : text/html

<HTML>
<HEAD>
<TITLE>RX sample</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFFF">
<FORM ACTION="/download.cgi" METHOD="post">
<TABLE BORDER=1>
<TR>
<TH>*215*355*217*234</TH>
<TH>SUBJECT</TH>
<TH>DATE</TH>
<TH>SIZE</TH>
<TH>Message-Id</TH>
</TR>
<TR>
<TD ALIGN=CENTER>
<INPUT TYPE="checkbox" NAME="D1">
</TD>
<TD>
<A HREF="image000.tif">IMAGE from Internet FAX</A>
</TD>
<TD>Fri, 19 Dec 97 21:48:32 JST</TD>
<TD>23134</TD>
<TD>395051913DE.EE58FOOHOG@Foo.co.jp</TD>
</TR>
<TR>
<TD ALIGN=CENTER>
<INPUT TYPE="checkbox" NAME="D2">
</TD>
<TD>
<A HREF="image001.tif">IMAGE from Internet FAX</A>
</TD>
<TD>Thu, 21 Oct 1999 16:34:30 +0900</TD>
<TD>56789</TD>
<TD>395053DC32.EE59FOOHOG@foo.co.jp</TD>
</TR>
</TABLE>
<P>
<INPUT TYPE="submit" VALUE="SUBMIT">
</FORM>
</BODY>
</HTML>

```

HTTP

HTML
文
字
列

【図14】

削除	SUBJECT	DATE	SIZE	Message-Id
<input type="checkbox"/>	<u>IMAGE form</u> Internet FAX	Fri, 19 Dec 97 21:48:32 JST	23134	395051913DE.EE58FOOHOGEEfoo.co.jp
<input type="checkbox"/>	<u>IMAGE form</u> Internet FAX	Thu, 21 Oct 1999 16:34:30 +0900	56789	395053DC32.EE59FOOHOGEE@foo.co.jp

SUBMIT

【図15】

●GETコマンドの例(受信データ要求)
GET/image000.tif HTTP/1.0
Referer : http://www.hoge.co.jp/rx.htm
Connection : Keep-Alive
User-Agent : foo/1.00
Host : www.hoge.co.jp
Accept : image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Authorization : Basic YXZjYzphdmNj
Cookie : SITESEVER=ID=09d0d169dc148c88b09862f78054e075

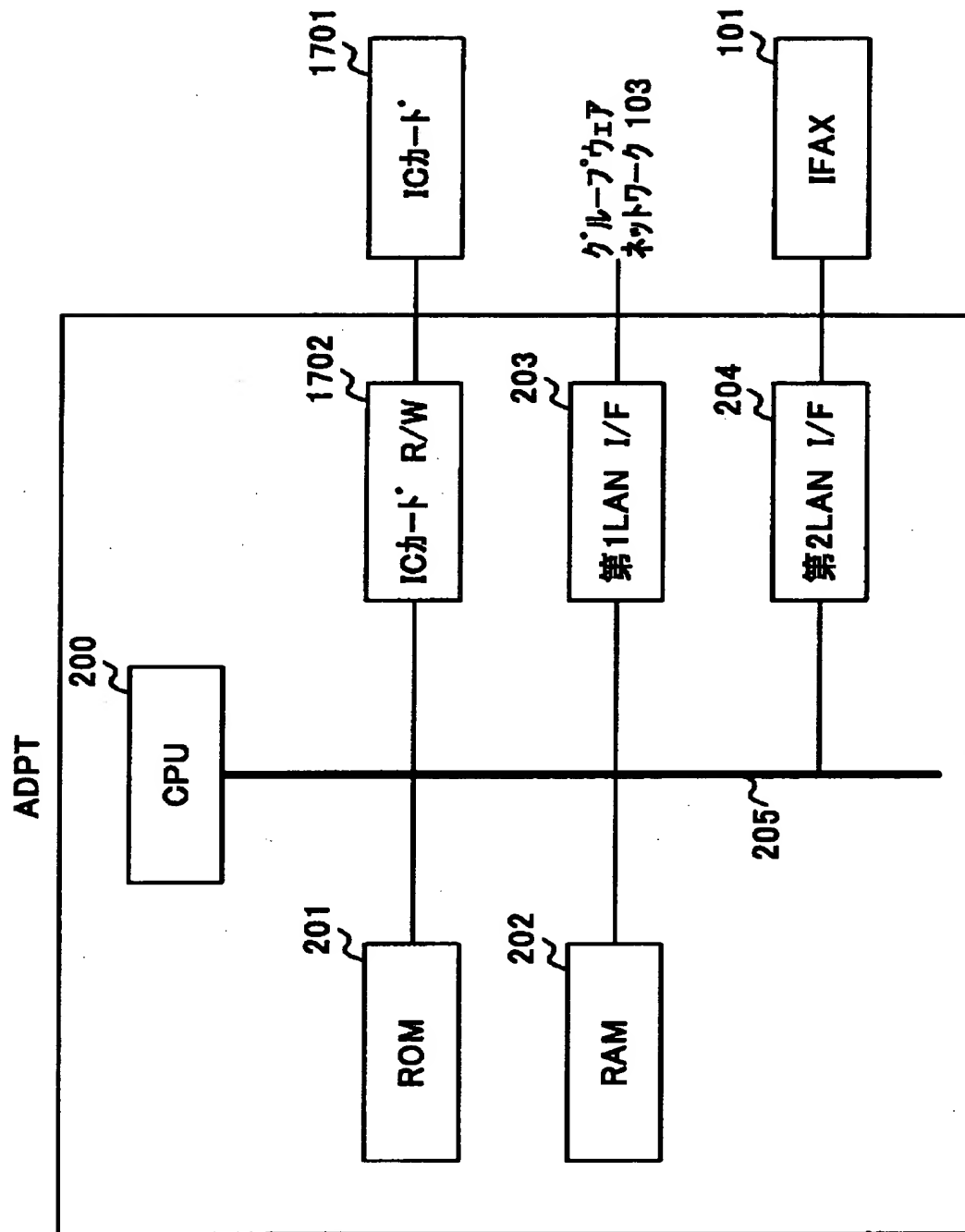
【図 16】

●POSTコマンドの例(削除要求)
 POST/download.cgi HTTP/1.0
 Referer : http://www.hoge.co.jp/rx.htm
 Connection : Keep-Alive
 User-Agent : foo/1.00
 Host : www.hoge.co.jp
 Accept : image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
 Authorization : Basic YXZjYzphdmNj
 Cookie : SITESEVER=ID=09d0d169dc148c88b09862f78054e075
 Content-type : application/x-www-form-urlencoded
 Content-length : 5

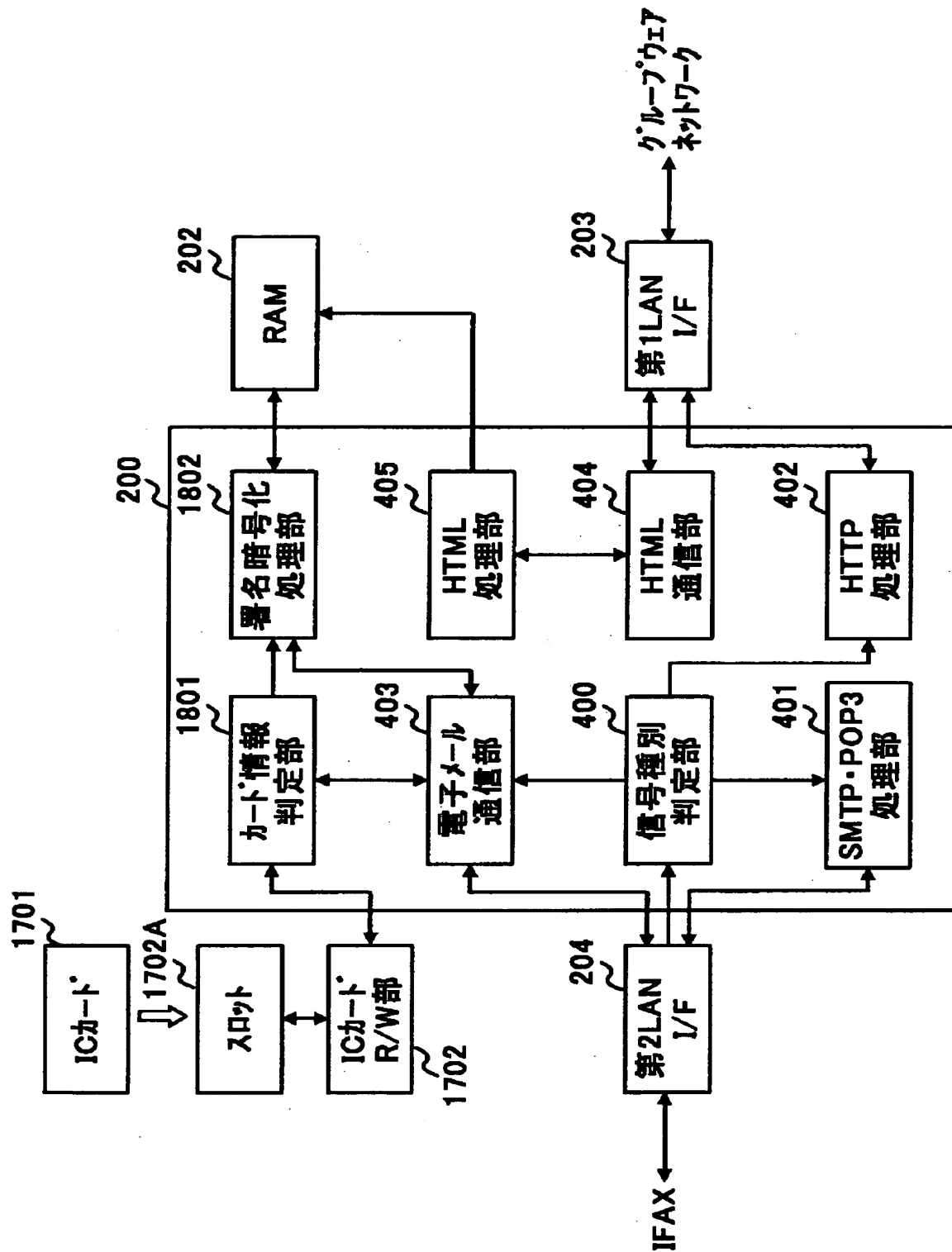
ヘッダ

送信データ [D1=on

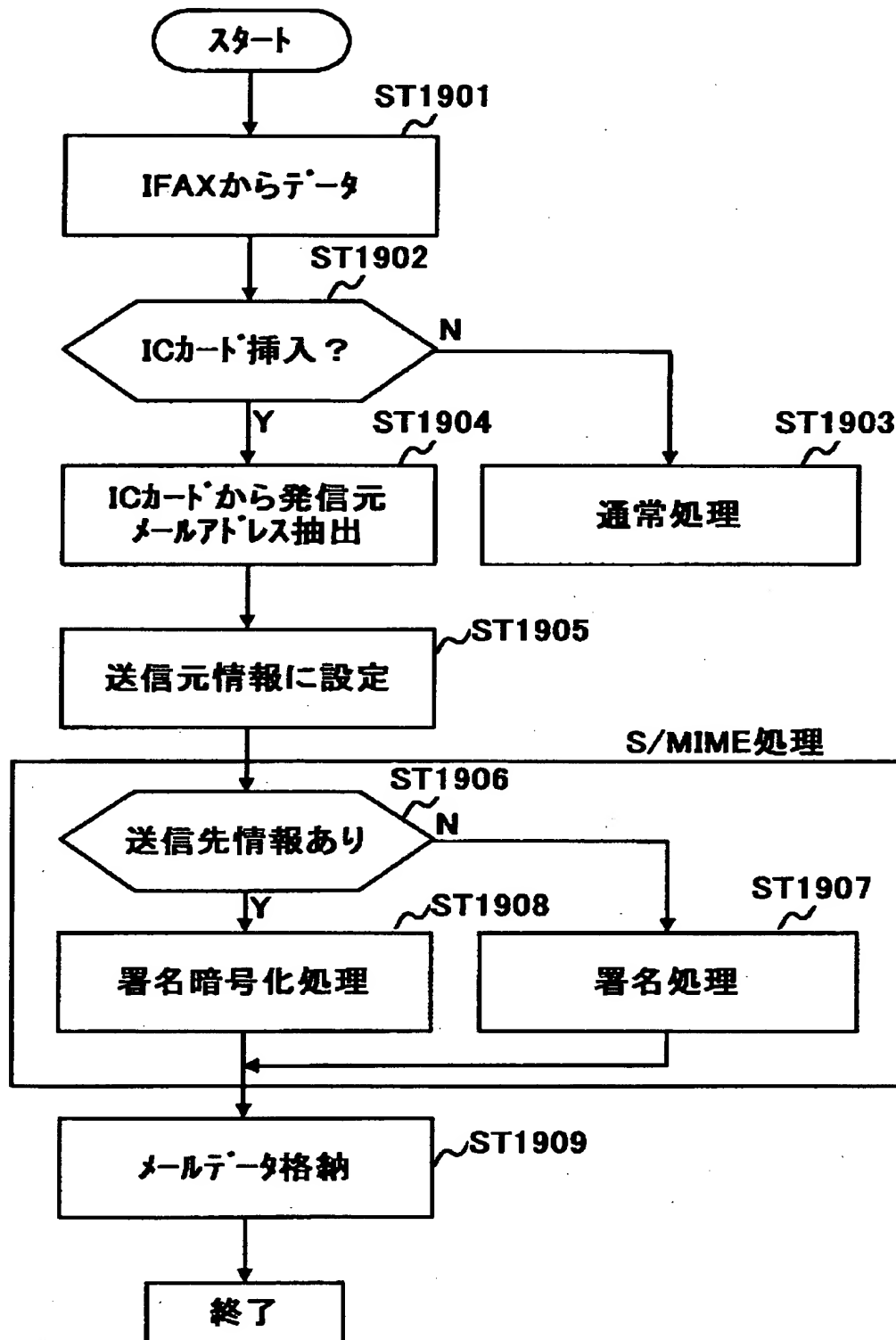
【図 17】



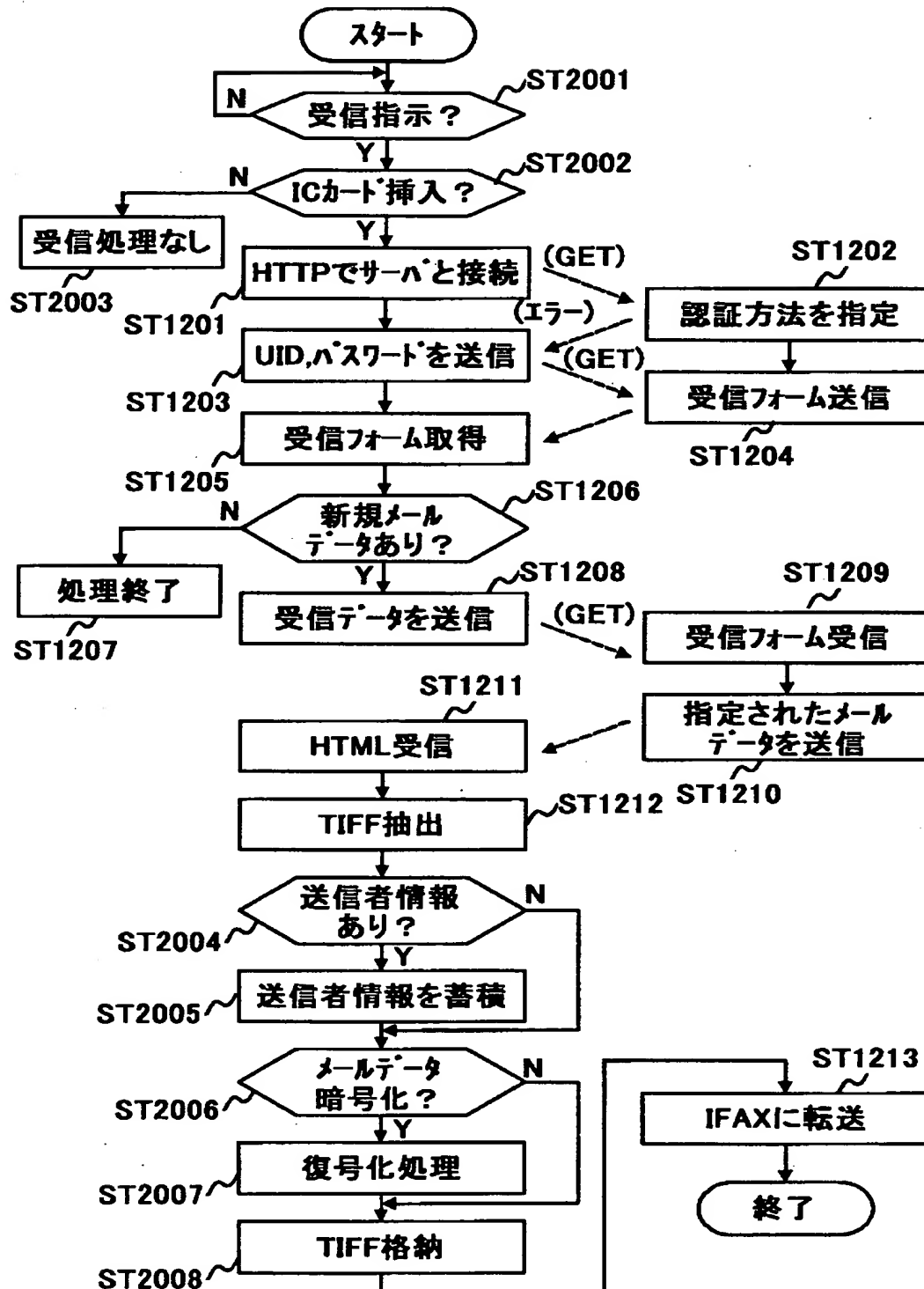
【図18】



【図19】



【図20】



【書類名】 要約書

【要約】

【課題】 HTTPプロトコルで管理されたネットワーク上でもI F A Xを正常に動作させること。

【解決手段】 信号種別判定部400がI F A X101に接続される第2 L A Nインタフェース204から送信される、S M T Pプロトコルに従った所定の信号種別をで判定する。所定の信号種別を判定した場合にI F A X101との間でS M T P・P O P 3処理部401がS M T Pプロトコルに従って通信を制御する一方、H T T P処理部402がグループウェアサーバ104との間でH T T Pプロトコルに従って通信を制御する。電子メール通信部403がI F A X101から受信した電子メールデータをH T M L処理部405でH T M Lデータに変換し、H T M L通信部404がそのH T M Lデータをグループウェアサーバ104に送信する。

【選択図】 図4

出 願 人 履 歴 情 報

識別番号 [000187736]

1. 変更年月日	1998年 4月13日
[変更理由]	名称変更
住 所	東京都目黒区下目黒2丁目3番8号
氏 名	松下電送システム株式会社